UNIVERSITY OF TORONTO

INFORMATION + TECHNOLOGY SERVICES

To: University Community
From: Robert Cook, CIO
Date: September 15, 2010

Re: Report #3 and Recommendations, Student e-Communications Services

In my May 12th, 2010 *Report #2 on Student e-Communications Services*, I recommended action to further evaluate the viability of an outsourced solution to meet the needs for student email services. Discussion at the May 20th PDAD&C meeting suggested additional actions.

I wish to report the outcomes of those investigations and my recommendation that the University now commence detailed discussions with a specific vendor, subject to certain conditions.

Actions recommended and taken, May 10th – August 19th, 2010

1. **That the University immediately develop and release a Request for Information (RFI) soliciting information from the supplier community on free outsourced options.**

I+TS immediately commenced a rigorous Request for Assistance (RFA) process recommended by Procurement Services to satisfy accountability requirements for an arrangement that would be seen as yielding value to the provider. The evaluation committee, chaired by Elizabeth Smyth, Vice-Dean Programs, SGS, consisted of students, faculty and staff drawn from the broad University community, many of whom had been on the earlier consultative committee. Responses for two "free" services, Google Apps and Microsoft Live@EDU, were reviewed. A third respondent offered a fee-based solution, and was consequently set aside.

The review confirmed that both respondents offered viable services incorporating the core requirements specified in Report #2, such as: email addresses would have the domain utoronto.ca; subdomains would be supported; features would include calendaring, collaborative groups, and multi-GB storage space; services would carry no advertising; data would not be not mined.

While strengths and weaknesses were different for each provider, both were deemed relatively comparable in a number of dimensions. These included:

- General data security provisions
  Judged likely better than current UTORMail standards; see Security Threat/Risk Analysis for details, Appendix 1.

- Protection of privacy
  Both providers store data on servers around the world; however risk may be made tolerable through notice to users; see Privacy Impact Assessment for details, Appendix 2.

CHIEF INFORMATION OFFICER
Simcoe Hall, 27 King's College Circle, Room 5K, Toronto ON M5S1A1 Canada
Tel: +1 416 978-8385 • Fax: +1 416 978-8903 • cio@utoronto.ca • www.its.utoronto.ca

- Potential for interoperability with other services
  Support for common standards.

- Administrative tools to support "incident management" by U of T administrators
  e.g., access to usage logs to support investigation of alleged inappropriate use.

- Accessibility features
  Both suppliers provide solutions compliant with contemporary accessibility standards.

Differences were noted in some areas, but not judged to be determinant:

- Onboarding and outboarding of accounts
  e.g., moving students to alumni status. It was anticipated that it would easier moving from one Google service to another i.e., alumni.utoronto.ca; but both solutions provide standard porting tools, and the continuation of alumni.utoronto.ca using Google services might logically come under review if student email moved to Live@EDU.

- Potential for future expansion of service to faculty and staff
  As Live@EDU runs on Exchange software, integrating with our existing Exchange services, if that were decided to be optimal, would be more transparent; however expansion of service to faculty and staff is likely doable with either solution.

This left just a few dimensions that emerged as deciding factors, each favouring one provider over the other, but in total split almost equally between the two competitors.

- Innovative features and rapid introduction of new tools
- User authentication protocol
- Profile within student community
- Potential for securing an acceptable contract
- Customer relationship reputation
- Breadth of existing and potential relationship with U of T
- Implementation costs
- Existing implementation know-how within University IT community
- Feature consistency and stability

The committee identified issues for follow-up investigation by I+TS staff, subsequently completed.

2. Continue consultation with the University community

a. Student survey

A 34 question survey on email use and future services was developed with the assistance of Student Life and delivered to 6000 undergraduate, graduate and professional students. The survey received 429 responses that closely paralleled the feedback received earlier from student members of consultative committees. A summary of responses can be found in Appendix 3.

b. Student organizations

With the assistance of Student Life, invitations to meet with project staff were sent to student organizations on all three campuses. A meeting with most student organization leaders scheduled for June 5th was cancelled for G20 related reasons. A drop-in session was held July 12th, and the Engineering Society executive arranged a follow-up consultation on July 26th. Feedback received aligned with survey and earlier consultation results. A meeting with members of the UTSU Executive took place September 3rd.

c. Faculty and staff

I+TS staff met with UTFA Council on May 20th. A meeting with three faculty members from Arts & Science and OISE was held June 10th to consider their security and privacy concerns, including trans-border information flow and intellectual property ownership. They asked that care be taken with respect to data storage, security and personal information privacy. They supported the proposed opt-out provision for students.

None of these community consultations revealed concerns beyond those raised during early study. Requirements with regard to security, privacy, improved functionality, bigger quotas and ease of use were consistently raised.

As we focus efforts on pursuing terms of a tentative contract, we anticipate additional direct engagement with students, faculty and staff as they take notice of the impending prospect of outsourced student email.

3. Continue analysis of privacy and security issues

Additional work was undertaken by the Information Security department of I+TS and the FIPP Office. The project's Privacy Impact Assessment has been revised in light of information acquired during the RFA process, as has the Security Threat/Risk Assessment. The latest versions are attached as Appendices 1 and 2. Notably, the documents continue to suggest that the security standards supported by the two outsourcing providers may well be tougher than what we can afford to do on our own, and that providing notice of risk to users is an important component of managing privacy responsibility, including Patriot Act vulnerability. Both documents will be further revised based on discussions with a specific provider.

4. Continue to monitor peer experience

We have continued to closely watch the efforts of University of Alberta to secure a contract with Google. Reports indicate few but very significant items are still outstanding as negotiations approach the twelve-month mark. The subject of the differences is unknown.

5. Additional legal consultation

We have identified external counsel experienced in outsourcing arrangements and kept Counsel up to date on developments. Counsel has suggested that a requirement to conclude language of a potential contract in 90 days would not be unreasonable.

6. Continue development of a communications plan

The project's end-user communications plan includes a website with project information and FAQs that are being tested.

7. That the CIO bring a specific recommendation with regard to outsourcing student email to the Principals & Deans meeting of June 24, 2010

The RFA revue process confirmed that both Google Apps and Microsoft Live@EDU are viable solutions for student email at U of T. Each solution presented different advantages – but committed to the economy offered by pursuing only a single solution, the prospects for concluding a satisfactory arrangement tipped the balance. Consequently, the CIO recommends that the University commence detailed discussion with Microsoft Canada toward implementation of **Live@EDU** as the institutional email service for students, subject to a number of conditions:

- that discussions to address the terms of service, concerns of either party, and potential contract language be concluded within 90 days
- that Microsoft work with the I+TS Information Security group to develop an acceptable authentication strategy that would not require passing id and password to Microsoft servers
- that Microsoft provide consulting support and staff training to achieve project implementation
- that the project's Privacy Impact Assessment and Security Threat/Risk Analysis be revised in anticipation of using Live@EDU and subsequently be judged acceptable to the University
- that any decision to proceed to execution of a contract to implement the Live@EDU service be subject to any community consultation required by the Vice-President & Provost.

With the cancellation of the June P&D meeting because of G20 arrangements, the consultation on the recommendation was delayed.

8. **That the University assign the institutional email accounts of students to a student designated domain, e.g. @student.utoronto.ca**

Feedback on this earlier recommendation revealed general support or neutral posture toward a distinctive domain name for student email accounts. Many, including a large number of surveyed students, however, felt that a blatantly transparent domain name was unnecessary, suggested classism, and could be disadvantageous to users. Alternatives have been considered, with the domain name @mail.utoronto.ca gaining most favour to date.

Next Steps and Timetable

Upon acceptance of the recommendation to proceed, the following schedule could be engaged:

Sept 24 on	Commence discussions toward achieving language for a potential contract Commence work to resolve authentication challenge Continue community consultation Develop project budget and scope of implementation plan
Oct 7	Update to Principals & Deans
Oct 21	Update to PDAD&C
~Nov 30	Conclude potential agreement details and authentication arrangement
Dec 9	Consultation with P&D (pending conclusion of a potential deal); solicit agreement in principle
~Dec 31	Sign agreement
Jan 1	Develop detailed implementation plan
Feb 1	Commence implementation with pilot group of students
May 2011	Commence production rollout to Spring/Summer session students
Sept 2011	Full scale rollout to students

UNIVERSITY OF TORONTO

Interim Threat / Risk Assessment

Student E-Communications Outsourcing Project

Martin Loeffler — Information Security, I+TS

Creation Date:	Version	1.0	June 24, 2010
Last Updated:	Version	2.0	July 6, 2010
	Version	2.1	July 6, 2010
	Version	3.0	July 12, 2010
	Version	4.0	Sept 22, 2010
	Version	4.1	Sept 22, 2010

Table of Contents

Executive Summary

The University of Toronto is exploring out-source options to replace its currently internally hosted and maintained student email system. As part of this exercise, an understanding of risks is required. These risks are not only to student email data, but potentially also to the reputation of the University itself.

The two vendors being considered to provide this out-sources service are Microsoft (via their Live@EDU product) and Google (via their Google Apps suite of web services). Both vendors are large, mature firms that are heavily invested in providing secure web-based services, and are unlikely to leave the marketplace.

On consideration of questions asked of both vendors, and an understanding of threats arising from legal, technical, and procedural sources, it is likely that out-sourcing email and associated services to either Google or Microsoft will result in reduced risk to student email data.

Sensitivity of Data to Risk

To clearly articulate risk to information, a Threat / Risk Analysis (TRA) is performed, identifying: data within the scope of the TRA; data sensitivity to risk of disclosure, loss, alteration, and unrecorded use or repudiation of receipt; agents or events that could cause such undesired outcomes to be realized; vulnerabilities that would enable threats to have an impact; and risk mitigation strategies that would address specific vulnerabilities.

The TRA regards 'security' as the effective and reliable mitigation of risk to confidentiality, integrity, availability and accountability for use of data, in the context of solution-specific vulnerabilities, and the sensitivity of data to risk.

Students have stated, via consultation, that they are prepared to accept known risks to the security of their data. This feedback has been confirmed through the University's observation of students' current practice of forwarding email out of the University of Toronto email system, to less secure systems such as Google mail, Hotmail, etc. As the practice of transferring email to an out-sourced solution already exists within the student population, the requirement for risk mitigation will be driven primarily by the data and usage requirements of official communications by the University of Toronto.

University of Toronto Data Usage

The University of Toronto currently uses email to communicate with students to achieve a variety of purposes: Communication in regards to accommodation of disabilities; academic censure, standing, and marks; financial matters; updates of personal / contact information; course requirements; and response to general queries. Given that these communications all take place via email, and that email between students is not separated from email between students and the University, all email must be regarded as being as sensitive as the most confidential of these communications. The sensitivities are as follows:

1. Communication in regards to accommodation of disabilities: Personally identifiable and health-related information - PHIPPA protected.

2. Academic censure, standing and marks; and, personal/contact information: Personally identifiable information - FIPPA protected.

Aggregate Sensitivity

Unless alternative arrangements are made in the handling of PHIPPA/FIPPA protected data, all email must be considered confidential and must be encrypted outside of the University of Toronto network. If PHIPPA/FIPPA protected data is removed from email sent by the University to students, while potentially private in nature from a student's point of view, the content of email is no longer classified by the University as confidential; while still requiring adequate access controls, non-confidential data does not require encryption outside of the University network.

Threat Scenarios

Threats in an email environment are many and varied, but are primarily the following:

1. Inappropriate access (disclosure / duplication / modification / deletion) to / of individual accounts
2. Loss of data in bulk
3. Loss of service
4. Lack of accountability for use

Given that each system under consideration provides the same basic functionality, using the same information (and absent system-specific architectural information), the threats to information are the same across all solutions.

Vulnerability Scenarios

System-specific vulnerabilities will be detailed after technology-level vendor discussions. Broadly speaking, vulnerabilities can be characterized as residing in the following areas:

Identification

In email, access identification is often the same as, or a portion of, a user's email address, which is communicated in clear text as part of the body of an email message; as such, access identifiers are low-sensitivity data, and the risk due to disclosure of access identifiers is low.

Authentication

Access credentials can be observed in transit, recovered from storage / memory, captured when input, or retrieved by administrators. As access credentials (i.e. passwords) are typically re-used many times before refresh, and provide full access to users' data when used in combination with easily-guessed access identifiers, access credentials are considered high-sensitivity data. As such, they must be protected from disclosure while in storage, transmission, use and administration.

Authorization

Account permissions are typically stored and administered by the service - vulnerabilities to account permissions are associated with vulnerabilities to system administrator access (Identification, Authentication and Monitoring). Management of system administrator-level vulnerabilities are tied to the reputational risk to the service vendor (discussed below, under 'Recommendations').

Isolation

In the absence of having unauthorized access to Identification and Authentication credentials, attempts may be made to circumvent access controls (typically through software vulnerabilities and / or social engineering attacks), so that possession of such credentials is not required to achieve unauthorized access to data. Management of access control-circumvention vulnerabilities are tied to the reputational risk to the service vendor (discussed below, under 'Recommendations').

Continuity

Loss of access to data may be temporary or permanent, depending on the vulnerability exploited. Management of continuity-level vulnerabilities are tied to the reputational risk to the service vendor (discussed below, under 'Recommendations').

Monitoring

Failure to monitor system and user activity severely limits the ability to trace / detect unauthorized service use, or attempts to circumvent access controls. Both Microsoft's and Google's solutions offer the University of Toronto the ability to provide its own activity monitoring, which is a requirement of the completed service architecture.

Risk Management Options

The Privacy Commissioner for Ontario has mandated that FIPPA and PHIPPA - protected data must be encrypted, when subject to risk of disclosure. Unless such information can be communicated to students other than via an outsourced email solution, that data must be encrypted - such an approach introduces issues of a technical nature, that are not currently fully resolved by currently available technical solutions. One possible alternative is to send notification of sensitive communications to students in an open email system, with the actual communication itself residing on a secure, University of Toronto - hosted and maintained system (such as Blackboard).

Exit Options

At the time of this writing, neither Microsoft nor Google explicitly support users exiting their service, they both do support account access via open standards such as POP and IMAP - conceivably an exit strategy could be built upon those protocols, allowing automated downloading of email data.

Residual Risks

All software has undiscovered weaknesses, and all procedures are subject to incomplete or non-observance; as such, risk is never completely eliminated. As well, the security of end-point devices is beyond the control of the on-line service provider; as such, unauthorized access to user accounts, singly or in bulk, should be anticipated.

Recommendations

Both vendors are subject to the provisions of the US PATRIOT act, however it is not clear, given reciprocal law-enforcement agreements between the United States and Canada, that hosting student email outside of Canada exposes that data to greater risk from governmental inquiry than at present. As the provision of web-based services is a large part of the business model for both firms, both firms are able to dedicate considerably more staff to the provision of a secure web-based service than any University or other educational institution; as such, the risk of unauthorized access due to technical or procedural vulnerabilities is likely to be less than at present.

Each platform offers sufficient functionality to satisfy the core requirements of the University of Toronto's intention to provide secure, reliable email to its students. As no security-level concerns invalidate either vendor, the decision between vendors will depend on additional functionality offerings, and, most importantly - as incident response depends on a vendor's willingness to engage - on the anticipated business relationship between the University of Toronto and the chosen vendor.

UNIVERSITY OF TORONTO

Interim Privacy Impact Assessment

Student E-Communications Outsourcing Project

Matthew Wilks, David Auclair — Information Security, I+TS

Howard Jones, Rafael Eskenazi — FIPP Office

Creation Date:	Version	1.0	April 16, 2010
Last Updated:	Version	1.02	April 19, 2010
	Version	1.03	June 11, 2010
	Version	1.1	June 21, 2010
	Version	1.11	June 22, 2010
	Version	1.12	June 23, 2010
	Version	1.13	July 7, 2010
	Version	2.0	Sept 22, 2010

Table of Contents

Executive Summary

A privacy impact assessment (PIA) is a process for determining and addressing privacy risk during the development and implementation of projects that involve or affect personal information. The PIA is an analysis of how project data flows align with legal, policy, practice and stakeholder privacy expectations. The PIA is a tool for executives to understand and address privacy risk in the project. This PIA is a living document that will continue to develop as the project develops. Future versions will align with milestones as the project develops.

As a result of a consultation on student e-communication, the CIO of the University has recommended "that at this point the University actively and aggressively pursue the single course of determining the best features and costs possible in an outsourced solution for student email." The two external service providers being considered are U.S. based: Google Inc. and Microsoft. The products under consideration are Google's *Apps for Education* and Microsoft's *Live@EDU*.

Both organizations attempt to relieve concerns surrounding what is perhaps the most talked about aspect of outsourcing email to an external provider: foreign legislation such as the Patriot Act in the United States. While the probability of such a request for information remains low, the risk to privacy it imposes – especially since Google or Microsoft might be forbidden from informing the user of such a request – is significant, with no possible mitigation.

While both organizations exhibit a high degree of attention to the privacy of their users, one possible area of concern lies in Google's statement that if they propose to use personal information "for any other purpose other than those described in this Privacy Policy", an effective opt-out would be provided[1]. It should be pursued whether the University could contractually bind Google to take an "opt-in" approach with the University's users. Both the respondents indicated that aggregate, non-personally identifying, statistical information would be collected and shared with third parties about the users of their services.

Once the service provider has been selected, the next step for the PIA is to perform a transactional level information flow analysis. Additional input from the service providers will be required in order to accomplish this. However, there is a high probability that the detailed interactions between the service providers systems will never be revealed to us.

[1] It should be noted that this "opt-out" only applies to Google's use of personal information. If Google wishes to share personal information with a third party, they state that they would require opt-in consent from the user.

Introduction

A privacy impact assessment (PIA) is a process for determining and addressing privacy risk during the development and implementation of projects that involve or affect personal information. A PIA typically contains a description of the project, a detailed transaction-level examination of data flows, and an assessment of how those data flows align with legal, policy, practice and stakeholder expectations. This analysis, together with possible mitigation strategies for identified privacy concerns, provides a tool for executives to understand and address privacy risk in the project. This PIA is a living document that will continue to develop as the project develops. Future versions will align with milestones as the project develops. The level of granularity will increase as we learn more about the detailed personal information transaction flows and will align with necessary decisions and risks associated with each milestone.

The University is committed to the requirements of the *Freedom of Information and Protection of Privacy Act* (FIPPA). In addition, since the third party contractor considered in this PIA is a private sector entity, adherence to *The Personal Information Protection and Electronic Documents Act* (PIPEDA) is necessary. Protection of privacy is not only a legal requirement but an integral element of projects involving personal information. Privacy protection is a necessary, responsible institutional practice in response to increasing threats to personal privacy.

Project Description

As a result of a consultation on student e-communication, the CIO of the University has recommended "that at this point the University actively and aggressively pursue the single course of determining the best features and costs possible in an outsourced solution for student email." The two external service providers being considered are U.S. based: Google Inc. and Microsoft. The products under consideration are Google's *Apps for Education* and Microsoft's *Live@EDU*.

Both of these companies offer a suite of tools that represent a "significant improvement to our status quo as well as support for some of the calendaring, document management and other communications integration aspirations discussed during the consultation." Since email has become an expected service at any institution, our email services are no longer a factor that differentiates the University. Students of universities that have switched to hosted email services have been happy with the additional storage capacity and features, while at the same time universities that have switched have been happy with the significant cost savings.

Special consideration must be given to the fact that in this case both of the external service providers are U.S. based corporations. The Ontario government publication, "*Guidelines for the Protection of Information when Contracting for Services*" attributes a very high risk to storage of sensitive information outside Canada, and a fundamental question of this assessment is how the University can meet privacy obligations and guarantee information security, privacy and control through contractual agreements. Equally central (if not more important) is the question of the reliability and trustworthiness of the external provider's reputation in the industry as well as the robustness and security of its hardware and software infrastructure. Care must be taken to ensure that the privacy of information is not an afterthought, but rather that privacy has been of central concern – with specific reference to the legislation governing the University – to the external provider at every stage of the development of its services and infrastructure.

In summary, the focus of this assessment will be to highlight risks to privacy in order to:

- Ensure that information that has been collected by the University is protected against unauthorized collection, use and disclosure in its exposure to an external service provider;
- Ensure that all information created or maintained through this project remains under the custody and control of the University; and
- Ensure that the external provider meets the requirements of the acts mentioned in the introduction to this document (FIPPA, PIPEDA), where / if applicable.

Bodies Involved

At this stage, the following bodies (corporate entities) are involved in this project:

- University of Toronto
  - Information + Technology Services
  - Freedom of Information and Protection of Privacy office
- Google Inc. or Microsoft, depending on the procurement process
  - Any and all sub-contractors to Google or Microsoft involved in the provision of the contracted services and who may have direct or incidental access to the personal information or records deemed to be under the control of the University

As this project develops, more entities may be added to this list.

Stakeholder Expectations

A committee was formed to solicit input from students about e-communications[2]. The committee met in person four times between November 2009 and January 2010. In addition to this there was an anonymous web form available on the I+TS website along with full information about the consultation. Many mediums were used to direct interested parties to the form including RSS feeds, Facebook, notices distributed by Student Life staff and email sent to the students at UTM.

Security and privacy were the most commonly raised concerns about outsourcing email to an external provider. Students who participated in the consultation expect and trust the University to appropriately protect their information. They did express concern about the misuse of information (e.g. data mining) and the communications channel (e.g. advertising) by an external provider. Concerns about the USA Patriot Act were also voiced. It was agreed that institutional negotiations with external providers would clarify and likely enhance security of data over that provided by the personal arrangements being made by individuals with these same providers.

[2] http://www.its.utoronto.ca/tri-campus_it/its_info/ITS_Comm_and_Consult/studentecomm.htm

Privacy by Design

Dr. Ann Cavoukian has developed a set of best principles surrounding the development of services that respect privacy called *Privacy By Design*[3]. We include these principles here as a reference point for discussions with vendors:

1. **Proactive** not Reactive; **Preventative** not Remedial

   The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the **Default**

   Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by *default*.

3. Privacy **Embedded** into Design

   Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. **Full** Functionality – Positive-Sum, not Zero-Sum

   Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretence of false dichotomies, such as privacy *vs*. security, demonstrating that it *is* possible to have both.

5. End-to-End Lifecycle Protection

   Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

[3] http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

6. Visibility and Transparency

   Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy

   Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Recommendation

Based on our analysis, we recommend that future discussions with possible student e-communications service providers take into account the following considerations:

Google

We should inquire if the University could contractually bind Google to take an "opt-in" approach for changes in the way they use our users' information, rather than "opt-out".

Microsoft

We should pursue talks with Microsoft under an additional NDA in order to supplement their RFA response with additional details.

It is necessary that notice be given to the end users of whichever system is chosen stating at least the following:

- User-supplied information will be stored on servers outside of the University's network, and may be subject to the US Patriot Act.
- That some products offered through the external provider (for example, Google Gadgets) may be offered with their own privacy policies. It would be up to the user to read those policies to make sure that they agree to the terms.
- And any additional terms as determined by the FIPP office, or I+TS.

The contract that is entered into by the University should address at least the following points:

- The external provider does not own the user data stored in its systems.
- The external provider cannot conduct data-mining on the user data.
- The external provider will not release any personal information to third parties unless required by law and where possible notify the University of any requests/demands for personal information.
- The external provider must support transport encryption for all communications between their data centres and users of their service.
- The external provider must perform audits regularly to ensure that they meet industry standard information security requirements.
- The external provider must notify us in advance of any changes to their privacy policy.
- The external provider should have an audited hardware disposal process.

APPENDIX 3:
QUICK SUMMARY: RESPONSES TO STUDENT QUESTIONNAIRE RE E-COMMUNICATIONS SERVICES

The survey received 429 responses to about 6000 invitations sent to undergraduate, graduate and professional students at the address listed in ROSI. Although this response rate is lower than for most Student Life surveys during the year, the consistency of responses provides some confidence in the results.

Responses confirmed the understandings we gained from student participants in the initial consultation on student e-communications services held from November 2009 – February 2010. These include the following (with % of respondents choosing a high or moderately important rating shown in parentheses.)

- Students want U of T to provide them with an email account (92%), one with an identifiable U of T domain name (90%)
- A large majority of respondents use their UTORmail account (91%), accessing it via a web browser interface (85%); but only one quarter consider UTORmail to be their primary email account.
- Fewer than one-quarter forward their UTORmail, predominantly to Gmail (46%)
- Nearly 2 in 3 respondents have only slight or no concern about security of the current U of T email service. Security concerns at a moderate to high level rise to over 50% when outsourcing is contemplated.

Respondents were asked to identify the new services or features they would like in a new service.
<u>The top ranked were:</u>

- Large storage quota (74%)
- Integrated personal calendar (54%)
- Online file storage (53%)
- Group mailing lists (49%)
- Online address book (49%)
- Enhanced security (46%)
- Enhanced privacy (44%)

Online productivity applications and website hosting ranked at the bottom. Asked for their highest priority, 40% said large storage quota, following next by 19% saying enhanced security.

Students were split on how concerned they would be with adoption of a domain to distinguish student accounts from staff and faculty accounts: 27% would be very concerned, and 36% not at all concerned. The most commonly cited reasons for concern were: additional length in the address and that labeling individuals as students would erode the prestige of their correspondence. Others argued that use of an explicit domain would unnecessarily reveal personal information.

The survey results are rich with data. If you wish more detail, including the many free-form comments submitted, please consult the survey data on our portal site.

Robert Cook, 24 June 2010

Simcoe Hall, 27 King's College Circle, Room 5K, Toronto, ON M5S 1A1 Canada
Tel: +1 416 978-8385 • Fax: +1 416 978-8903 • its@utoronto.ca • www.its.utoronto.ca