MICROSOFT OFFICE 365 PRIVACY IMPACT ASSESSMENT

Western Student E-Communications Outsourcing

Paul Eluchok – University Privacy Officer

David Ghantous – Associate Director of Technical Services

Dated: August 19, 2014

Student Email Migration to Microsoft Office 365

Privacy Assessment

Background

Western's Information Technology Services (ITS) selected Microsoft Office 365 as a new email solution for students. The plan is to move student email accounts to this service provided by Microsoft. Microsoft Office 365 will provide students with not only email, but additional services and tools including email and calendar integration.

The current student email system (Convergence) is an 'on premises' solution that is managed and maintained by ITS. As the need for student mail has evolved since Western's first implementation of Convergence, Western has outgrown its own platform, resulting in higher maintenance costs and numerous deficiencies relative to the changing needs of the student. In short, the current solution is at end-of-life. Over that same time, the availability of robust and high quality external service providers has grown. These providers offer extremely cost-effective solutions with greater capacity, improved availability and access, enhanced security and a variety of features not available in Western's current environment.

The move to using an external, third-party email system was evaluated by ITS, Legal Counsel and the Privacy Office. The objectives of this consultation were to determine if there was the requirement to complete a Privacy Impact Assessment (PIA) on the project, and to seek advice and recommendations to ensure Western's compliance with The Freedom of Information and Protection of Privacy Act (FIPPA). This Act requires Western to ensure that reasonable measures are taken to prevent unauthorized access to the records taking into account the nature of the records to be protected.

Email in Canadian Education

Email has seen a significant shift in recent years. As the availability of inexpensive or even free solutions has expanded, so has the dependence on email for the regular business of universities. Other channels (e.g. Twitter, Facebook) have also grown in usage, but the need for email has continued to increase, resulting in increased cost for universities.

The commoditization of the service along with the increasing costs of in-house solutions has resulted in many universities shifting to 3rd party providers like Google and Microsoft. Thousands of universities worldwide have outsourced email services, including many in Canada. As the level of adoption of cloud email services has increased, the experiences of other institutions are proving to be invaluable. These include Canadian universities like Queen's, University of Toronto, Dalhousie, Lakehead and Carleton. The University of Alberta has successfully migrated student, staff and faculty email to Google. In fact, a majority of Canadian universities are either moving or are considering a move to cloud based email for students. Those that have started the migration have assessed the privacy implications to the students and deemed the solutions to be acceptable for delivering this service. Being a late entrant in the cloud email space affords Western the opportunity to benefit from the experiences of others through consultation at both the technical and legal levels.

Privacy Impact Assessment (PIA)

The objectives of this PIA are to determine if there are privacy issues or risks associated with the outsourcing of student email, and if so, to provide recommendations and mitigation strategies. ITS, in conjunction with legal counsel, the Privacy Officer and the Security Officer have conducted an assessment of privacy concerns. The assessment included a careful review of the existing campus agreement, privacy legislation, Western's policies, consultation with peer institutions and a variety of other sources, both internal and external to Western. In addition, the configuration and the authentication model for Microsoft Office 365 were designed with these considerations in mind. This assessment finds that Microsoft's physical and logical controls align with University privacy policy in the context of student email.

As such, it was determined that Microsoft Office 365 for students does not present major privacy risks to Western.

Any remaining risk should be mitigated or limited through the implementation of strategies and recommendations developed as part of this exercise. In addition, the Privacy Officer and Security Officer should remain an integral part of the project through to its completion.

1. **Recommendation**: *Western's Privacy Officer and Security Officer should be included as members of the Microsoft Office 365 implementation team for the duration of the project.*

Solution Overview

While Western's current solution has email data and credentials stored (at rest) on premises, the Microsoft Office 365 solution will result in email data being stored on Microsoft's premises. Western's credentials, however, will remain (at rest) on Western's premises. The significant change between the two systems is that email would be stored on Microsoft's servers (as opposed to Western's server) and email between Western Student Users while now cross the internet (where as previously it was only processed on Western's server).

The following Figure 1 represents the current flow of data for student email.

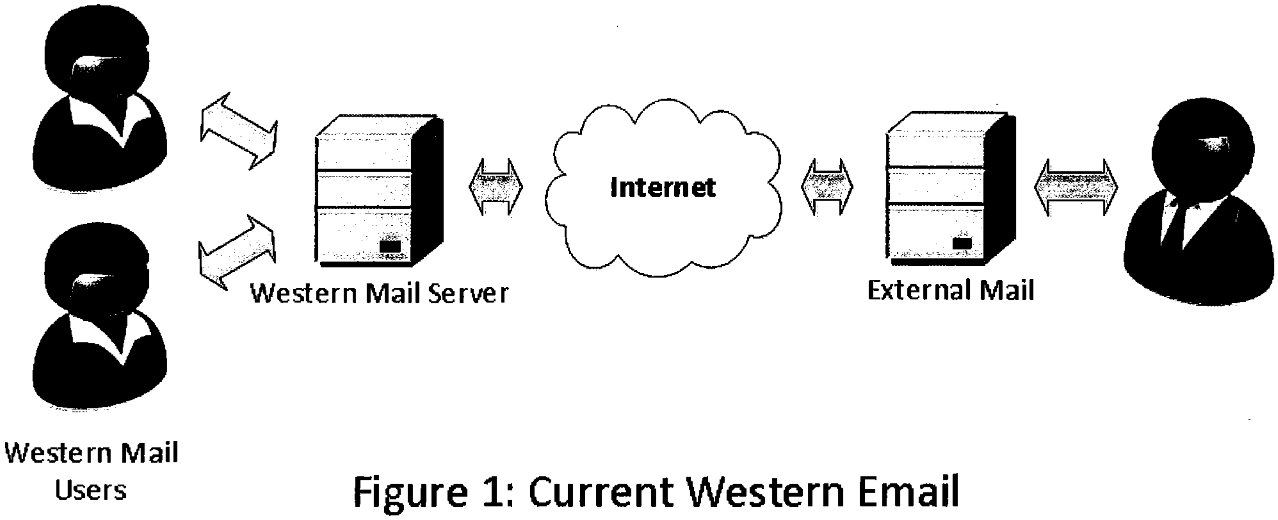

Figure 1: Current Western Email

The following figure 2 represents the flow of data for student email under Microsoft 365.

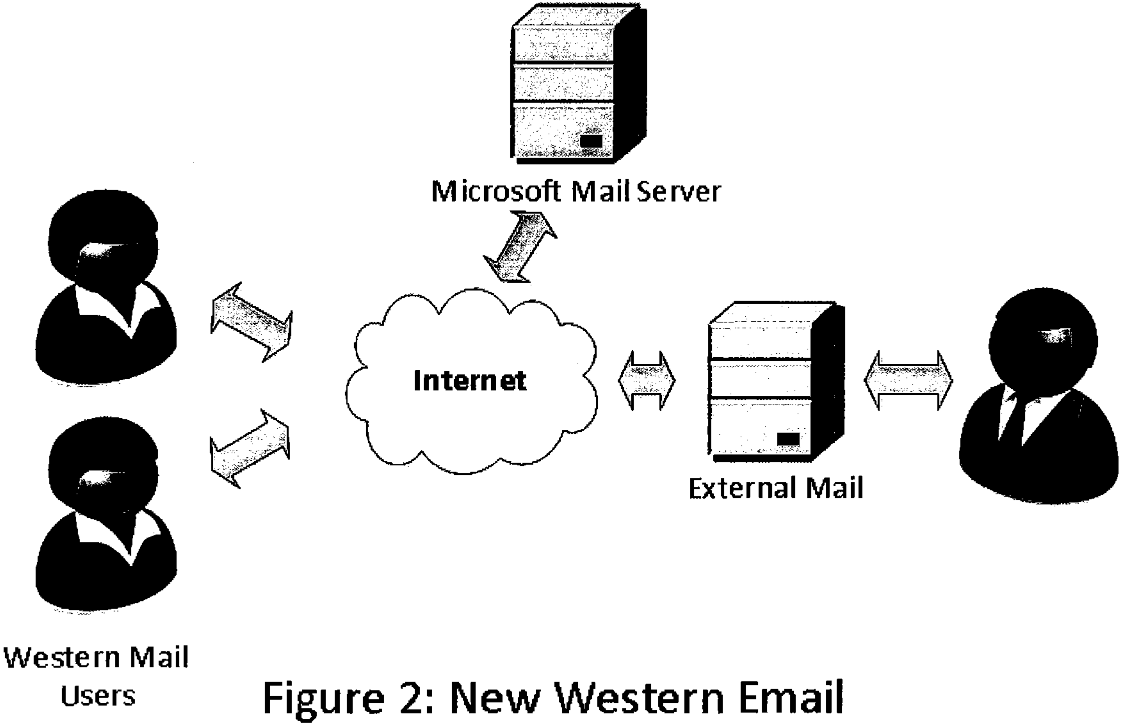

Figure 2: New Western Email

Authority for Collection, Use and Disclosure

Western's privacy obligations originate from the Freedom of Information and Protection of Privacy Act (FIPPA), which permits Western to collect, use and disclose personal information necessary for the proper administration of the university and its services. Except in limited and specific circumstances, Western must collect personal information directly from the individuals the information is about and must provide notice of the collection.

ITS will be accessing and using information already collected by other central administrative sources at Western. Microsoft Office 365 will be linked with certain systems controlled by Western for the sole purpose of account set-up and authentication.

All Western students will be automatically eligible for a Western email account starting from the time they apply to Western and through to the time at which they are no long registered as a student. As an alumnus, they will then be eligible for an Alumni account which is out of scope of this project and this assessment. The purpose of these accounts is to ensure that students have a constant and consistent means of receiving information related to their studies and Western in general.

The system will be designed to ensure that the minimum amount of personal information will be disclosed by Western to Microsoft both during the setup/migration process and ongoing.

The planned disclosure of information to Microsoft is as follows:

o Student name
o Student enrollment details (group membership)
o Assigned email address

Microsoft Office 365 will store the following information:
o Student name
o Student enrollment details (group membership)
o Student email address
o Student email data

2. **Recommendation**: *Western should ensure that only the minimum amount of personal information is used to create student email accounts and that any changes or considerations regarding the collection, use and disclosure of information are in compliance with privacy legislation, and that the principles of 'minimum amount' and 'need to know' are considered and applied.*

Considerations for Student Email Data

It is the position of Western that student email is not information that is considered under the custody or control of Western and therefore FIPPA does not apply to this information. It is not considered information collected by Western for use by Western for its purposes. However, the information in the email system is considered the personal information of the student and the system should be designed to protect it to the same security standards that would apply to any other university system that contains personal information.

Location of Information

Microsoft's primary data centres for Western student mail are in the United States. FIPPA does not prohibit personal information from being stored in another province or country. In Privacy Investigative Report PC12-39, the Ontario Privacy Commissioner noted that FIPPA does not prohibit provincial institutions from outsourcing services, including outsourcing services outside of the province or even outside of Canada. The critical question for institutions such as Western is whether they have taken reasonable steps to protect the privacy and security of the records in their custody and control. Whether personal information is held in Canada or internationally, the primary responsibility and obligation of Western under FIPPA is to ensure that reasonable security safeguards are in place to ensure the secure collection, use, retention, disclosure and disposal of personal information.

To ensure accountability, Western has negotiated a Master Campus Agreement with Microsoft, which includes provisions related to ownership of data; collection, use and disclosure of information; notice of compelled disclosure; breach notification; security; retention and disposal of student information; subcontracting to third parties; the audit of Microsoft's systems; and governing law of the Master Campus Agreement.

Further, Microsoft has numerous privacy and security features designed to protect student data. Its security measures surpass those offered by Western. That being said, regardless of whether a student is using Western's system or Microsoft's system, email has inherent risk. There is always a risk that student data could be intercepted by third parties or even foreign countries. For example, the United States Patriot Act permits the US government to legally intercept data in certain circumstances. Where confidentiality is imperative, students should be warned that other methods of sharing data should be considered.

3. **Recommendation**: *Students be notified in advance of claiming their email that their information will reside in a foreign jurisdiction and will be subject to the laws of that jurisdiction, and that the University cannot guarantee protection against possible disclosure of personal information that is held in foreign jurisdictions.*

4. **Recommendation**: *Western should implement an on-premises data exchange solution so that sensitive information can be securely shared.*

Information Controls

Microsoft's Master Campus Agreement with Western addresses information controls. In particular, the Agreement provides:

- Microsoft is not the owner of the data stored on their systems
- Microsoft will not release any personal information to third parties unless required by law and, where legally permitted, Microsoft will notify Western of any requests/demands for personal information.
- Microsoft will support transport encryption for all communications between their data centres and users of their service.
- Microsoft will perform audits regularly to ensure that they meet industry standard information security and privacy requirements and share such audits with Western upon request
- Microsoft will notify us in advance of any changes to their privacy policy.
- Microsoft will not conduct data mining on user data.

In addition, consideration for data retention and processes to ensure that data which is no longer needed is purged must be a part of the email implementation.

5. **Recommendation**: *ITS should work with Microsoft to ensure that unclaimed and unused student email accounts are not held in perpetuity to ensure that the minimum amount of information is held on Microsoft's system.*

6. **Recommendation**: *ITS should request the annual audit report from Microsoft to determine whether any issues have arisen which affects the security and privacy of student data.*

Security

Microsoft stores the data of millions of customers worldwide. As such, security is an integral feature to its success. In almost every aspect of data protection, Microsoft equals or exceeds that of Western. Its facilities are heavily protected and its security procedures are identified in the Master Campus Agreement and under constant review. Microsoft constantly monitors its infrastructure to ensure its security and privacy controls are effective. While Microsoft security controls and management processes are designed to reduce the risk of security incidents, they can still occur. Microsoft therefore employs a Security Incident Management (SIM) team to respond to attacks, 24 hours a day, 7 days a week. The SIM has a 6 phase incident response process which includes training, identification, containment, mitigation, recovery and analysis of lessons learned. In the event that Microsoft becomes aware of any unlawful access to any student data stored on Microsoft's equipment or in Microsoft's facilities; or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of student data (each a "Security Incident"), Microsoft will promptly (1) notify Western of the Security Incident; (2) investigate the Security Incident and provide Western with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Companion Products

As part of the Microsoft Office 365 student email enrollment and the Microsoft Master Campus Agreement, students may have the opportunity to make use of other cloud-based, value-added products. While providing email and calendaring for students may enable access to these products, these additional services may include their own privacy agreement or terms of use. Students must ensure that they have read and are familiar with these terms prior to making use of these products.

The Privacy Impact Assessment process to-date has considered privacy compliance solely with the migration of student email to Microsoft Office 365. Other tools such as SharePoint, which allow for group collaboration, may be utilized by students and the privacy, security and records management functionality were not assessed under this document.

Finally, Western may choose to make use of the capabilities of either calendaring or email in day-to-day operation. For example, academic calendars could be used to automatically populate student calendars. As with all processes involving private or sensitive data, Western must assess risk and ensure compliance with FIPPA.

7. **Recommendation:** *Western should consider a staged implementation of Microsoft Office 365 for students, starting with email. A separate assessment of other cloud based tools should be undertaken as they are introduced.*

8. **Recommendation**: *Western should conduct additional Privacy Assessments when instituting processes that may present inherent risks to student privacy. Western should issue separate communications to students relating to any/each of these processes as a key outcome of these additional Privacy Assessments.*

The Role of the User in Privacy and Security

Western and Microsoft are not alone in their responsibility to safeguard the privacy and security of student identity and sensitive or private information. It is also the responsibility of the student to ensure that they are careful to protect their password. In accordance with Western's policies, their password should be known only to them and never shared. There are no processes either within Western or Microsoft whereby they would be asked to reveal their password for any reason.

It should also be noted that email, whether on premises or in the cloud, is not a natural vehicle for highly sensitive or private data. The sending of this type of data over email provides an opportunity for that data to fall into the wrong hands either through mismanagement or intentional interception.

9. **Recommendation:** *Students should be advised to treat their email as confidential and not to share their password with anyone, including ITS or any other Western department, for any purpose. Clear communication on the importance of protecting themselves and reading and understanding the Terms of Use must be a part of the communication strategy for this project and moving forward.*

10. **Recommendation**: *All students should be presented with and asked to agree with the Microsoft Terms of Use as well as Western policy statements on privacy and computer resources prior to their final enrolments in Office 365.*

11. **Recommendation**: *Microsoft Office 365 Terms of Use statement be reviewed by legal counsel to ensure all necessary elements are included.*

Staff and Faculty

Staff and Faculty are not within the current scope of this Privacy Impact Assessment and/or migration to a new email platform. It has been decided that faculty and staff email will remain within the existing environment of Western for this phase of the project. This creates some complexity as the roles of individual constituents are not always clear - a number of students have dual roles and are also members of the staff.

Students are frequently hired by Western in a variety of positions. The overlap in roles between student and staff will need to be explored further in relation to privacy, security and administration. This may result in the inclusion of some staff or the exclusion of some students as the planning and design process progresses.

12. **Recommendation**: *Western should assess privacy, security and administrative provisions between the Microsoft Office 365 email system for students and the internal Microsoft Exchange email system for faculty and staff to determine how individuals with dual or multiple roles will be assigned within each system.*

Conclusion

The implementation of Microsoft Office365 for student email presents limited risk for Western and should proceed. A series of mitigation strategies should be developed through the implementation of the recommendations outlined in this document. They are:

1. *Western's Privacy Officer and Security Officer should be included as members of the Microsoft Office 365 implementation team for the duration of the project.*

2. *Western should ensure that only the minimum amount of personal information is used to create student email accounts and that any changes or considerations regarding the collection, use and disclosure of information are in compliance with privacy legislation, and that the principles of 'minimum amount' and 'need to know' are considered and applied.*

3. *Students be notified in advance of claiming their email that their information will reside in a foreign jurisdiction and will be subject to the laws of that jurisdiction, and that the University cannot guarantee protection against possible disclosure of personal information that is held in foreign jurisdictions.*

4. *Western should implement an on-premises data exchange solution so that sensitive information can be shared privately and securely.*

5. *ITS should work with Microsoft to ensure that unclaimed and unused student email accounts are not held in perpetuity to ensure that the minimum amount of information is held on Microsoft's system.*

6. *ITS should request the annual audit report from Microsoft to determine whether any issues have arisen which affects the security and privacy of student data.*

7. *Western should consider a staged implementation of Microsoft Office 365 for students, starting with email. A separate assessment of other cloud based tools should be undertaken as they are introduced.*

8. *Western should conduct additional Privacy Assessments when instituting processes that may present inherent risks to student privacy. Western should issue separate communications to students relating to any/each of these processes as a key outcome of these additional Privacy Assessments.*

9. *Students should be advised to treat their email as confidential and not to share their password with anyone, including ITS or any other Western department, for any purpose. Clear communication on the importance of protecting themselves and reading and understanding the Terms of Use must be a part of the communication strategy for this project and moving forward.*

10. *All students should be presented with and asked to agree to the Microsoft Terms of Use as well as Western policy statements on privacy and computer resources prior to their enrolments in Office 365.*

11. *Microsoft Office 365 Terms of Use statement be reviewed by legal counsel to ensure all necessary elements are included.*

12. *Western should assess privacy, security and administrative provisions between the Microsoft Office 365 email system for students and the internal Microsoft Exchange email system for faculty and staff to determine how individuals with dual or multiple roles will be assigned within each system.*

Additional Resources

White paper on Microsoft Privacy:
http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=28540

Microsoft Trust Centre:
http://office.microsoft.com/en-ca/business/office-365-trust-center-cloud-computing-security-FX103030390.aspx