Privacy Impact Assessment

Microsoft Office 365 Implementation: Student email project

Background

University of Manitoba, Information Services and Technology (IST), has selected Microsoft Office 365 as a new email solution for students. The primary goal of the project is to move student email accounts to a service provided by a third party. It is also the intention to provide all alumni and retirees with a lifelong UM email account. Microsoft Office 365 will provide students with not only email, but also additional services and tools including email and calendar integration, the Microsoft Office Suite, and collaboration and communication tools such as SharePoint and Lync.

The current student email system is an in-house supported, open-source system. It is also used to create email accounts for retirees, and other University associates that may require temporary UM email addresses. Over the years, student email needs have changed significantly and the current system has become a challenge for IST to manage and maintain. The ability to offer an in-house email system that is congruent with student needs has proven to be cost prohibitive. Moving student email to an external service provider not only provides a cost-effective solution, it also provides greater storage, improved availability and access, enhanced security, excellent reliability, and a variety of office and collaboration tools that would be highly utilized by students.

The move to using an external, third-party email system was evaluated by IST and the Office of Legal Counsel and the Access and 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 the University of Manitoba's compliance with *The Freedom of Information and Protection of Privacy Act* (FIPPA) and *The Personal Health Information Act* (PHIA). These Acts put strict limits on the collection, use and disclosure of personal information and personal health information by a public body under FIPPA, or Trustee under PHIA. The guiding principle provided by the legislation is to limit the collection, use and disclosure of personal and personal health information to only the minimum amount required for a specific, stated and authorized purpose.

Privacy Impact Assessment (PIA)

The objectives of a PIA are to determine if there are privacy issues or risks associated with a project, and if so, to provide recommendations and mitigation strategies. It was determined that a PIA should be undertaken on the project. Staff from IST completed the questionnaire and they were readily available to answer questions and discuss potential risks and possible mitigation strategies. The PIA was completed in conjunction with the review and negotiation related to the proposed Microsoft Office 365 contract. It proved very valuable to connect the two processes as the University has been able to strengthen the privacy provisions contained in the contract in a substantial way.

Based on the work completed to-date, the Access and Privacy Office can confirm that the privacy of students is of foremost importance to the University and IST. The system set-up and migration will reflect this understanding and ensure that sufficient controls are in place internally to ensure privacy is protected. Microsoft Office 365 does not present major privacy risks to the University if the risk

mitigation recommendations from this report are implemented and if the protection of privacy remains a priority throughout the lifetime of the project.

> **Recommendation**: *The Access and Privacy Office should be included as a member of the Microsoft Office 365 implementation team for the duration of the project.*

Authority for Collection, Use and Disclosure

The University is authorized by *The University of Manitoba Act* and FIPPA, to collect, use and disclose personal information to establish and carry-out approved functions of the University. The University is required to collect personal information directly from the individuals the information is about and must provide contact information of someone within the University that can answer questions about the collection, use and disclosure.

IST will be accessing and using information collected by a central administrative source at the University. Microsoft Office 365 will be linked with other University systems for the purpose of account set-up and identity authentication. The systems that contain or will contain personal information that have been in scope for the PIA process include Banner, Iridium, Active Directory and Microsoft Office 365.

All University students will be automatically eligible for a University email account and they will claim their account through Iridium. The same user name and password will apply to logging in and using a number of systems at the University such as Jump and Desire2Learn. It will be essential for current students to claim and maintain a University email to ensure they receive information and also access to University systems.

The system will be designed to ensure that the minimum amount of personal information will be disclosed and stored outside of the University to Microsoft to set up the student email system. The planned disclosure of information to Microsoft is as follows:

Iridium will connect with Microsoft Office 365 to transfer the following information:

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

Microsoft Office 365 will store the following information:

- Student name
- Student enrollment details (group membership)
- Student email address
- Student email content*

> **Recommendation**: *The University 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.*

Recommendation: *The University ensure that a secure and safe process is established, tested and implemented to transfer information from Banner to Iridium and ultimately to Microsoft Office 365.*

*The content in student email is not information that is considered under the custody or control of the University and therefore *The Freedom of Information and Protection of Privacy Act* (FIPPA) does not apply to this information. It is not considered information collected by the University for use by the University for business purposes. The email system is also not designed to collect personal health information for use by the University and therefore *The Personal Health Information Act* (PHIA) does not apply to the content of student email. However, the information in the email system is considered sensitive information and the system should be designed to protect the information to the reasonable security standards that would apply to any other University system that contains sensitive personal information.

Recommendation: *Students be notified to treat their email as confidential and not to share their password with anyone.*

Recommendation: *Students be notified to not use the email system to send or receive sensitive personal health information.*

Recommendation: *Privacy and notification statements be written and included in the new system for all students to view prior to using the system.*

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

Control, Security and Integrity of Information

One of the most challenging problems in any information management system that contains sensitive information is the complex issue of ensuring that appropriate controls and security are applied to maintain the integrity and confidentiality of the information.

Recommendation: *Microsoft be contractually obligated to comply with applicable privacy laws, including restrictions related to the collection, use, disclosure, retention and disposal of personal information.*

Recommendation: *Microsoft be contractually obligated to maintain reasonable security standards to protect and back up data in the system.*

Recommendation: *Microsoft be contractually obligated to immediately notify the University of any unauthorized access to the system or other confirmed breach of security.*

Location of Information

Microsoft provides global online services with data centres located throughout the world. Manitoba law does not prohibit personal information from being held in another jurisdiction, including the United

States. It is recognized that many leading suppliers of information technology are global companies, often with headquarters in the United States and data centres in other jurisdictions. Canadian organizations, including universities, are seeking cost effective, efficient and secure technology solutions to improve business processes. This means that, at times, vendors in locations outside of one's own jurisdiction may need to be considered.

Whether personal information is held in Manitoba, Canada, or internationally, the primary responsibility and obligation of the University is to ensure that reasonable security safeguards are in place to ensure the secure collection, use, retention, disclosure and disposal of personal information, and that all practices in place are in compliance with Manitoba access and privacy laws.

The University should be transparent about their information handling practices and ensure that individuals using the system understand where their personal information is being held.

> **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 jurisdiction.*

Records Management

Records Management broadly refers to the systematic control of the creation, receipt, maintenance, use and disposition of records (destruction or transfer to archives). Under FIPPA, a record is defined as a "record of information in any form, and includes information that is written, photographed, recorded or stored in any manner, on any storage medium or by any means, including by graphic, electronic or mechanical means." The University has a records management program in place that provides assistance for faculties, departments and offices to design Records Authority Schedules that govern the retention and destruction of both paper and electronic records.

The University has Records Authority Schedules in place to manage student information held by the University in systems of authority such as Banner. The content in student email accounts will not be managed by the University. Additionally, the content created through the use of other Office 365 tools, such as Outlook and Word, will also not be managed by the University.

It is vital, however, to ensure that the accounts created for students are set up and maintained properly and in compliance with FIPPA.

> **Recommendation**: *Change requests, such as a name change or spelling correction that are approved and implemented by the Registrar's Office in Banner should be updated in the Microsoft Office 365 system so that the information is always current.*

> **Recommendation**: *IST work closely with the vendor to ensure that regular maintenance of the Microsoft Office 365 system takes place and that unclaimed and unused student email accounts are not held in perpetuity to ensure that the minimum amount of information is held in the system.*

Other Recommendations

The Privacy Impact Assessment process to-date has considered privacy compliance primarily with the migration of student email to Microsoft Office 365. This product provides a wide-range of tools, some of which would potentially require the use of a greater amount of personal information to set up and implement. For example, the integrated calendaring program could allow a student's academic calendar including class and lab times to be populated into the Microsoft Office 365 calendar tool. Other tools such as SharePoint, which allow for group collaboration, may be utilized by both staff and students and the privacy, security and records management functionality were not assessment by this PIA. Therefore, further recommendations relevant to the implementation of the Microsoft Office 365 system that should be noted include:

> **Recommendation:** *The University should consider a staged implementation of Microsoft Office 365 for students, with email being the first provision, and with other tools being reviewed to ensure compliance with Manitoba privacy law.*
>
> **Recommendation**: *If the University considers populating student academic calendars into the Office 365 calendar, a privacy review should be done to ensure compliance with Manitoba privacy law.*
>
> **Recommendation**: *Expanded future use and all updates, upgrades and enhancements to Microsoft Office 365 should be examined and evaluated in relation to compliance with Manitoba privacy laws.*

It should also be stated that faculty and staff email will not be moving to Microsoft Office 365 as a part of this project. It has been decided that faculty and staff email will remain within the managed environment of the University. This division may create challenges during the migration to Microsoft Office 365 due to the fluid nature of staff and student roles at the University. Students are frequently hired by the University in a variety of positions such as Grader-Marker, Instructor and staff member in an office such as the Registrar's Office. The overlap in roles between student and staff will need to be explored further in relation to privacy, security and administration.

> **Recommendation**: *The University 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.*

Finally, using Microsoft Office 365 to provide email services for alumni and retirees in addition to students may prove to be administratively and technically challenging as the needs among the groups are different. There is also the additional challenge of providing temporary University email accounts for associates during specific joint projects with other universities or organizations such as joint admissions committees.

> **Recommendation**: *The University should consider a staged implementation of Microsoft Office 365 for groups such as alumni and retirees and engage with internal stakeholders to review the needs and potential uses of the system for each group.*
>
> **Recommendation:** *The University consider using the internal staff email system for the creation of temporary email accounts.*

Conclusion

This privacy risk assessment includes nineteen (19) risk mitigation recommendations relating to the migration of student email to Microsoft Office 365. The recommendations are summarized on the following pages and may serve as a Privacy Risk Management Plan for the project.

Privacy Risk Management Plan (Summary of Recommendations)

The following provides a summary of the recommendations regarding the implementation of a new student email solution:

1. **Recommendation**: *The Access and Privacy Office should be included as a member of the Microsoft Office 365 implementation team for the duration of the project.*

2. **Recommendation**: *The University 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. **Recommendation**: *The University ensure that a secure and safe process is established, tested and implemented to transfer information from Banner to Iridium and ultimately to Microsoft Office 365.*

4. **Recommendation:** *Students be notified to treat their email as confidential and not to share their password with anyone.*

5. **Recommendation**: *Students be notified to not use the email system to send or receive sensitive personal health information.*

6. **Recommendation**: *Privacy and notification statements be written and included in the new system for all students to view prior to using the system.*

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

8. **Recommendation**: *Microsoft be contractually obligated to comply with applicable privacy laws, including restrictions related to the collection, use, disclosure, retention and disposal of personal information.*

9. **Recommendation**: *Microsoft be contractually obligated to maintain reasonable security standards to protect and back up data in the system.*

10. **Recommendation**: *Microsoft be contractually obligated to immediately notify the University of any unauthorized access to the system or other confirmed breach of security.*

11. **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 jurisdiction, in accordance with the laws of that jurisdiction.*

12. **Recommendation**: *Change requests, such as a name change or spelling correction that are approved and implemented by the Registrar's Office in Banner should be updated in the Microsoft Office 365 system so that the information is always current.*

13. **Recommendation**: *IST work closely with the vendor to ensure that regular maintenance of the Microsoft Office 365 system takes place and that unclaimed and unused student email accounts are not held in perpetuity to ensure that the minimum amount of information is held in the system.*

14. **Recommendation:** *The University should consider a staged implementation of Microsoft Office 365 for students, with email being the first provision, and with other tools being reviewed to ensure compliance with Manitoba privacy law.*

15. **Recommendation**: *If the University considers populating student academic calendars into the Office 365 calendar, a privacy review should be done to ensure compliance with Manitoba privacy law.*

16. **Recommendation**: *Expanded future use and all updates, upgrades and enhancements to Microsoft Office 365 should be examined and evaluated in relation to compliance with Manitoba privacy laws.*

17. **Recommendation**: *The University 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.*

18. **Recommendation**: *The University should consider a staged implementation of Microsoft Office 365 for groups such as alumni and retirees and engage with internal stakeholders to review the needs and potential uses of the system for each group.*

19. **Recommendation:** *The University consider using the internal staff email system for the creation of temporary email accounts.*