Executive Summary

This assessment finds that Microsoft’s physical and logical controls align with University security policy and privacy obligations and that any remaining risk should be mitigated or limited through the implementation of strategies and recommendations developed as part of this exercise. However, this assessment should be conceived as an ongoing and iterative exercise rather than a one-time event. There should be an annual review to determine current best practices, to ensure the implementation of mitigation strategies and to review the success of such strategies.

Part 1:
Overview of the e-Communications Migration to Microsoft Office 365

Background

Western Technology Services (WTS) selected Microsoft Office 365 as e-communications service for students, faculty and staff. Microsoft Office 365 provides Western users with not only email and calendar services, but additional services and tools such as OneDrive, a file hosting service. For the purpose of this assessment, Microsoft’s services shall be collectively referred to as “Microsoft Office 365”.

Prior to the Microsoft Office 365 email and calendar migrations, all email and calendaring services offered by Western (Convergence) were through an ‘on premises’ solution that was and remains managed and maintained by WTS. As the need for email and calendar services evolved since Western’s first implementation of Convergence, Western outgrew its own platform, resulting in higher maintenance costs and numerous deficiencies relative to the changing needs of students, faculty and staff. 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 service was evaluated by WTS, Legal Counsel and the Privacy Office. The objective of this consultation was to determine if there existed 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) and to prevent unauthorized access to user data taking into account the nature of the data to be protected.
As of the date of this version of the assessment, several significant events have occurred which led to the revisions to the assessment.

First, students were transitioned to the Microsoft Office 365 service without incident in February, 2015. Second, the articles “Seeing through the Cloud” and “Privacy Impact Assessments and Microsoft & Google Vendor Contracts” have been published and identify important considerations to address in this assessment. Third, Microsoft announced on June 2, 2015, that it would open two new data centers in Canada as part of its network of data centers outside of the United States. Fourth, non-academic staff were transitioned to Microsoft Office 365 at the end of December, 2015. Fifth, Microsoft opened its Canadian data centers in Toronto and Quebec City in 2016 and advised Western that Western had the option to have its email and other data hosted in Canada; Western exercised that option and is awaiting the transfer of its data to these Canadian data centers, which transfer is anticipated to occur by the end of 2018. Sixth, in the spring and summer of 2016, Western migrated email for faculty to Microsoft Office 365; as Western’s Microsoft Office 365 data was stored in the United States, faculty were offered the option, on an individual basis, to delay the migration of their email and calendar accounts until all of Western’s Microsoft Office 365 data was hosted in Canada. In the fall of 2016, the decision was made by the WTS steering committee to provide faculty and staff access to Microsoft OneDrive due to requests from individual faculty and staff members. Microsoft OneDrive has been implemented for students. In December of 2017, Microsoft notified Western that all mail and data for Western now resides in Canadian Data Centres and faculty who opted to delay the migration will now be required to migrate.

e-Communications Solutions in Canadian Education

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

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

Cloud Storage Solutions in Canadian Education

Similar in many ways to e-communications, storage has shifted toward commodity cloud based solutions. The availability of very large and often free storage spaces has resulted in a shift to these platforms that can be accessed, through the same login as email, from any location where there is a computer/tablet/handheld device and an internet connection.

Microsoft Office 365 offers a solution called Microsoft OneDrive. Microsoft OneDrive is a file hosting service that gives users the ability to sync files and later access them from a web browser or mobile device. Users can also choose to share files with other individuals, whether they be Microsoft Office 365 users or not. The storage limited for OneDrive users is currently one terabyte, but this may change without notice.

Several universities have provided or are in the processing of providing their faculty and staff access to Microsoft OneDrive including Queens, McGill, and Dalhousie. The provision of a service such as OneDrive provides university faculty and staff with significant flexible and personalized storage capabilities while curbing the use of other file sharing services which have not been reviewed or otherwise authorized by Western, such as DropBox or a file sharing service offered through a faculty or staff member’s personal email account, such as GMail’s Google Drive.

The Objectives of this Privacy Impact Assessment (PIA)

The objectives of this PIA are to determine if there are privacy issues or risks associated with the outsourcing to Microsoft Office 365, and if so, to provide recommendations and mitigation strategies. WTS, in conjunction with Legal Counsel and the Privacy Office have conducted an assessment of certain 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.

Western’s Privacy Obligations and How Microsoft Office 365 Uses Personal Information
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. Under its regulations, FIPPA requires Western to ensure that reasonable measures to prevent unauthorized access to the records are defined, documented and put in place, taking into account the nature of the records to be protected.

Three types of personal information will be shared with, collected and used by Microsoft in delivering Microsoft Office 365. The first type of information is authentication and identification information, which is information used by Microsoft to facilitate authentication and identification of each user. This includes the user’s Western email address, the user’s full name, and a Microsoft token.

The second type of information is user-created content, which refers to information in the user’s profile, emails, calendar and information the user places in Microsoft Office 365. This information is created by the user and may be personal, administrative, research-based or educational.

The third type of data is system-captured content, which refers to data collected by Microsoft from users using technologies like cookies, and receiving error reports or usage data, which is used to improve the solution and to store a user’s preferences and settings.

**How does Data Flow through the Office 365 Solution?**

Users accessing Microsoft Office 365 must log in through a web portal managed by Western. The user is authenticated on Western’s campus through ADFS (Active Directory Federated Services) before accessing the services which are operating on Microsoft’s servers. At no time are user credentials stored at or validated by Microsoft.

Following successful authentication, data transactions occur directly between the user and Microsoft.

The important differences between the Convergence system and Microsoft Office 365 is that user data is stored (at rest) on Microsoft’s servers (as opposed to Western’s server) and email between Western account holders while both users are on campus using an Ethernet connection will cross the internet (where as previously the data was only processed on Western’s internal network).

The following Figure 1 represents the flow of data for email and calendar data in the Convergence system.
The following figure 2 represents the flow of data for email and calendar data under Microsoft 365.

How does OneDrive Data Flow to and from the Office 365 Solution?

Through the same login used to access their email, users will have the option to use Microsoft’s file sharing service, Microsoft OneDrive. For Microsoft Office documents (Word, Excel, PowerPoint) users are able to create, edit and save documents online without having to download them. Users may also upload and download non-Office documents using OneDrive. In all cases, files can be
upload and downloaded by the user at the user’s option, subject to the storage restrictions imposed by Microsoft.

The following represents this interaction:

Figure 3: Western Cloud Storage
Part 2:
Understanding the Privacy Implications

Data and Data Minimization

A core principle of privacy protection is the use of information only as necessary to fulfill the stated purpose. The Microsoft Office 365 solution should therefore collect, use and disclose a minimal amount of the user’s personal information to achieve the solution’s purpose.

With regard to authentication and identification data, the user’s name and email address are provided to and collected by Microsoft. However, Microsoft is never provided with a user’s password. Authentication is implemented and confirmed by Western, as identity provider, and therefore user identification, registration and authentication remains solely with Western. Western provides an authentication token to Microsoft as a confirmation that the user is valid and then Microsoft grants the user access to the solution.

The users control their user-created content and the content which they receive from others, including the deletion of such content. Western’s policies on the proper use of computing resources, security, privacy and access to information, the student code of conduct, and its collective agreement obligations continue to apply to these activities and to the content which users generate. Users should be notified that these obligations continue to apply within Microsoft Office 365, though Western does not audit for compliance.

System-captured content received by Microsoft is information that Microsoft collects from users and logs during operation of Microsoft Office 365. Microsoft’s Privacy Policy outlines the type of information collected, how it will be used and how a user can control and limit the use of this data.

Western’s WTS department respects the rights of users’ privacy, in accordance with university policies and relevant legislation. WTS will not access a user’s account unless they are investigating a case of system abuse or otherwise acting in accordance with a law enforcement investigation. At such times, they will notify the user of the actions taken, the reasons and the findings.

Access to data may occur at the request of law enforcement officials or due to legal process (i.e. subpoenas). Both Microsoft and Western have processes in place to carefully review, validate and respond to lawful access requests. The user may be notified of such access unless it would compromise the investigation or the law or court order prohibits such notification.
**Data Destruction**

The user’s user name and password is deleted when a user’s account is deleted, usually at the option of the user. User generated content is controlled by the user and can be deleted at any time. System-captured content may be retained indefinitely by Microsoft.

Within 30 days of a user’s account being deleted, all data associated with the user’s account is permanently deleted from Microsoft’s storage. It is not persisted at Western or Microsoft or anywhere else. The data no longer exists. This policy can be modified through archiving and hold procedures and settings which are configurable by Western.

Upon termination of the Microsoft Agreement, Western will have 90 days to export all data from Microsoft before it is destroyed.

**Location of Information**

With the exception of user passwords, all data is stored at Microsoft’s datacenters. Microsoft Office 365 is a cloud based service, meaning the application and data is hosted on a network of servers. When Western first moved to Microsoft’s mail platform, we selected the United States as its primary storage region. In June, 2015, Microsoft announced that it was developing datacenters in Canada to be located in Toronto and Quebec City. These data centres opened in early 2016. And, as of December 2017, all of Western’s data now resides in these two data centres.

**Security & Service Continuity**

Microsoft’s Office 365 complies with the following control standards and frameworks: ISO 27001, ISO 27002 Code of Practice, ISO 27018 Code of Practice, SSAE 16 SOC 1 Type II, and SSAE 16 SOC 2 Type II.

In terms of physical security, Microsoft restricts physical data center access to authorized personnel and has implemented multiple layers of physical security, such as biometric readers, motion sensors, 24-hour secured access, video camera surveillance, and security breach alarms.

In terms of electronic security, Microsoft enables encryption of data both at rest and via the network as it is transmitted between a data center and a user.
Microsoft’s service continuity process is to replicate the data and Microsoft Office 365 platform across multiple servers housed in multiple data centers in the primary data region; this process enables simple data reconstruction from an alternate data centre and it also causes minimal, if any, service disruption if a catastrophic event occurs at one particular datacenter.

For more information on Microsoft’s security practises, see Microsoft’s Online Service Terms at http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31

And Microsoft’s Trust Center at: https://products.office.com/en-ca/business/office-365-trust-center-cloud-computing-security

Security Breach Protocols for both Microsoft and Western

If Microsoft becomes aware of any unlawful access to any user data stored on Microsoft’s servers or in Microsoft’s facilities, or unauthorized access to such servers or facilities resulting in loss, disclosure, or alteration of user 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. Notification(s) of Security Incidents will be delivered to one or more of Western’s administrators.

*It is recommended as a protocol that in the event of a Security Incident, Western’s WTS department would notify its Directors, its Campus Information Security Officer and Western’s Privacy Officer. These individuals would then work together to investigate and monitor the Security Incident, review any reports received from Microsoft, ensure satisfactory resolution of the incident, and issue a report to the Provost. Depending on the nature of the breach, Western would also notify affected users.*

Audit Reports

Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing user data (including personal data), as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for the solution.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
• Each audit will be performed by qualified, independent, third party security auditors at Microsoft’s selection and expense.

Each audit will result in the generation of an audit report (“Microsoft Audit Report”), which will be Microsoft’s confidential information. The Microsoft Audit Report will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor. If Western makes a request for a copy of the Microsoft Audit Report, Microsoft will provide Western with the Microsoft Audit Report so that Western can verify Microsoft’s compliance with its security obligations. Western should therefore periodically request copies of these audit reports to monitor Microsoft’s compliance with security standards.

User Privacy

With limited exceptions, users can control how their data is displayed, used, shared, and destroyed. Although users are not able to change their email address, users do control their email and when it is destroyed, subject to access to information and retention laws and policies. Users are also in control of their calendar and are able to control who can view their calendar information; by default, student, faculty and staff calendars will display busy and free information only. When using Microsoft’s OneDrive, users control when individual files are created, shared and destroyed.

Contact information presently found in Western’s online directory is also uploaded to Microsoft. Faculty and Staff names and email addresses are uploaded to Microsoft. Student names and email addresses are also uploaded unless the student has requested to opt-out of the directory through Western’s Registrar’s Office. Certain staff and faculty are also not listed in the directory due to the sensitivity of their role or through special arrangement.

Microsoft does not serve advertisements to its educational users of Microsoft Office 365, which is a practise in contrast to its commercial accounts.

At this point in time, Microsoft Office 365 will be the only centrally supported solution offered by Western to its students and non-academic staff. Faculty and academic staff have also migrated to Office 365, however a small number remain in Convergence until such time as Western is able to move their data into the Microsoft system, now resident in Canada, and Convergence is disabled. No new faculty or academic staff accounts will be created in Convergence. Students are provided with a Microsoft Office 365 account while students at Western and the account is/will be used as the official mode of communication with students. Students will continue to have access to Office 365 email for life, but will lose access to OneDrive once they cease to be a student. Staff and faculty will be
provided with a Microsoft Office 365 account while employed by Western. Within 300 days of the end of their employment with Western, their Office 365 account will be closed. When an account is closed, the data associated with that account is deleted. It may take up to 30 days for the data to be permanently deleted.

In terms of educating users on privacy, Microsoft has a privacy policy, which can be found online here: [https://privacy.microsoft.com/en-ca/privacystatement](https://privacy.microsoft.com/en-ca/privacystatement). Western’s WTS department has also published information on the solution here: [http://www.uwo.ca/its/email/index.html](http://www.uwo.ca/its/email/index.html).

**Data Classification Standards**

Western established a standard framework for classifying Western data based on its level of sensitivity, value and criticality to the University as required by the University’s Information Classification Standards. Classification of data aids in determining baseline security controls for the protection of data.

These standards map out three levels or classes of Data:

1. **Confidential** – If compromised in some form or fashion, is likely to result in significant and/or long-term harm to the institution and/or individuals whose data it is.
2. **Sensitive** - when released without authorization, could be expected to cause minor, short-term harm or embarrassment to the institution and/or individuals whose data it is, and is intended for only limited dissemination.
3. **Public Data** - Public data which is readily available to any member of the Western University community or to the general public, either upon request or by virtue of its being posted or published by Western University through its proper administrative procedures.

*For both email and OneDrive, it is recommended that the user use alternative services in the handling of confidential data or alternatively secure the data through strong encryption. The use of Email or OneDrive for the storage and dissemination of confidential data unnecessarily exposes data to risk that can be avoided through the use of other platforms and services.* Consequently, Faculties and departments should inventory the types of data in their custody and control, identify confidential data commonly in their custody and control, and determine whether these services should be used for the transfer and storage of such information, and, if so, the parameters for such use. For example, a Faculty should determine whether documents related to a student’s medical accommodation request should be shared in OneDrive; a principal investigator should determine whether human participant data related to Research Ethics protocol should be sent as an attachment.
by email; and a department such as Advancement & Development should determine whether donor data or human resource data related to its employees should be stored in OneDrive.

*When using these services for sensitive data, it is recommended that users assess the need and appropriateness for the transfer and storage of such data using these services and delete data that is no longer needed.* Similar to confidential data, each Faculty and Department at Western should identify types of sensitive data commonly in its custody and control and determine whether the services should be used in relation to that data.

**Part 3:**

**Identifying Risks and Mitigating Risks through Solutions**

**Loss of Direct Management and Control**

**Risk**

The loss of direct management and control of user data is considered a significant risk. Microsoft would be in possession of data belonging to users of the service. By design therefore, there are certain risks, including:

1. Unauthorized disclosure of user data, including personal information;
2. Unauthorized use by Microsoft of user information or information about a user’s use of the service;
3. Users being subject to unwanted services and solicitations;
4. Unauthorized retention of user data;
5. Inability to independently resolve service failures;
6. Inability to independently access data on demand; and
7. Inability to independently restore lost or corrupted data.

**Solutions to Mitigate Risks**

Microsoft Office 365 offers far more comprehensive and robust security controls and continuity than that provided by the Convergence system. However, neither Microsoft nor Western can guarantee
the security of information, whether in transit or at rest. Consequently, Microsoft has agreed to notify Western in the event that it becomes aware of any unauthorized disclosure affecting a Western user, to investigate such disclosure and report on it to Western, and to take reasonable measures to mitigate the effects and to minimize any damage resulting from the disclosure.

In accordance with the Online Service Terms, user data can only be used by Microsoft to provide Microsoft Office365 and Microsoft has agreed not to use user data or derive information from it for any advertising or similar commercial purposes. The user retains ownership of all of the user’s data stored by Microsoft.

When a user deletes information on Microsoft 365, Western has thirty days during which it can recover the message through its administrator after which the information is permanently deleted.

By entering into the agreement with Microsoft and moving to a cloud based service, Microsoft will host and manage the data of the Microsoft Office 365 users. However, Microsoft offers a better service in terms of resolving service failures, service continuity and the ability to restore lost and corrupted data. Microsoft guarantees an up time of 99.9%, maintains emergency and contingency plans for its facilities and has a redundant storage system and procedures for recovering data designed to attempt to reconstruct user data in its original or last-replicated state from before the time it was lost or destroyed.

Important privacy and security features are contained within documents that are subject to change such as Microsoft’s privacy policy and its online service terms. Consequently, Western should constantly review the most current versions of these documents to determine whether any changes have an unacceptable impact on it and its users.

From a business continuity perspective, best practices suggest that Western should maintain a plan for a transition to another system in the event that the relationship with Microsoft unfavourably changes. Such a plan would help to mitigate the risks associated with unacceptable changes, which could include changes in cost, changes in Microsoft’s privacy policy or changes related to risks of unauthorized disclosure.

Access by Foreign Governments

Risks
Microsoft Office 365 is a cloud based service, where user information is stored in Microsoft’s datacenters around the world. Western has selected Canada as its primary storage region for data at rest. According to Microsoft, it has two datacenters located in Quebec City and Toronto. Microsoft replicates customer data in these two datacenters for reliability and availability. If a datacenter ceases functioning for any reason, user data is not lost as the application software and user data running on that application software are also available from the second datacenter. Western or its users might not be notified when failover occurs. Depending on the particular service, failover may not result in any service interruption. Western and its users should assume that, at any given time, their data is being processed in either one or both of the datacenters in Canada.

This does not mean, however, that user data will not leave Canada. According to Microsoft, the requirements of providing the services may mean that some data is moved to or accessed by Microsoft personnel or subcontractors outside of Canada. An example provided by Microsoft is that to address latency, routing data may need to be copied to different datacenters in different regions. In addition, personnel who have the most technical expertise to troubleshoot specific service issues may be located in locations other than Canada, and they may require access to systems or data for purposes of resolving an issue.

**Solutions to Mitigate Risks**

As analyzed above, although there is a risk of government surveillance, the risk has a very low probability. Despite this, mitigation measures should still be put in place to further reduce the probability of the risk from occurring.

*The University should notify the users at the time of registration about where their information is stored and that their information will be subject to the laws of that jurisdiction. They should also be notified about secure alternatives to Microsoft Office 365, where available. This will give users the information needed to make an informed choice about using Microsoft Office 365.*

*It is also recommended that Western educate its Microsoft Office 365 users on the risks associated with e-communications and cloud storage and the benefits of using secure repositories to store and manage confidential and highly-sensitive information. Western should continue to establish on-premises solutions for the sharing of sensitive information between Western faculty and staff, such as an on-premises Sharepoint solution, as this would provide a secure transfer of information, which would not leave Western’s servers.*

*Western’s Microsoft Office 365 administrators should ensure that they receive compliance notifications from Microsoft. These notifications will provide updates if there is a change to the*
information regarding Office 365 geographic boundaries, as well as changes to Microsoft’s security, privacy, and compliance program.

**Student Calendars**

**Risk**

Staff, faculty and students will have access to online calendar through Microsoft Office 365. Western will also have the functionality to import faculty members and student class schedules into the users calendars. Currently, this functionality is being used by Ivey.

As mentioned, these calendars will automatically show when a user is busy or free to another Western user but not provide any further information unless the user has chosen to share the calendar information with another user inside or outside of Western. If the user chooses to share the calendar information with another user, the other user is able to add to the calendar directly and, depending on the permission, the other user is able to view the calendar, to edit it, or to act as the user’s delegate for meeting requests.

The ability to view when a student is busy or free reveals personal information about a student and goes against the principle of privacy by default. By looking at a student’s calendar, a person would be able to identify when the student was likely on campus or off-campus, which reveals something of a personal nature about the student.

**Solutions to Mitigate Risk**

*It is recommended that, if possible, student user calendars not be accessible to anyone unless the student has granted express permission.*

**Email Directory**

**Risk**

Western publishes an online email directory that contains entries for every student, faculty and staff member at Western. When an individual becomes a student, faculty or staff member of Western, the individual is automatically added to the directory. A student has the option to opt out of the directory. Certain staff members are not added to the directory due to the sensitivity of their role or through special arrangement.

Western has imported this directory into its current e-communications solution and it is accessible to all users. It is the intention to import the directory into Microsoft Office 365.
Whereas a faculty or staff member’s email address would not be considered personal information, a student’s email address would be considered personal information. By accessing the student directory, one is able to determine whether an individual is a current student of Western thus revealing information relating to his or her education. Further, if a student is enrolled at a faculty with a specialized email address such as Ivey, Schulich or Engineering, one is able to obtain even more information about the student’s education.

Solutions to Mitigate Risk

The current protocol allows students to opt out of the directory, which protocol is identified on Western’s Registrar’s website under Student Records, Updating Personal Information. It is recommended however that either Western remove students from the directory or that it notify students as part of the Microsoft Office 365 account set up process that their email address will be part of a publicly accessible directory and the student has the ability to opt out of the directory by utilizing the protocol on the Registrar’s website.
Part 4:
Additional Resources

Western`s Data Classification Standards:
http://security.uwo.ca/information_governance/standards/data_classification/index.html

White paper on Microsoft Privacy:

Microsoft Trust Centre:

“Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World,” (2015) by Heidi Bohaker, Lisa Austin, Andrew Clement and Stephanie Perrin