



July 17, 2020

Privacy & Information Security Impact Assessment Report

Online Proctoring: Respondus

Trudi Wright, Privacy & Records Management Specialist
Privacy Office (University Secretariat)

Background

Before COVID-19, McMaster University instructors administered the majority of examinations in-person. COVID-19 presented an academic challenge in teaching and learning remotely – in particular, it is not possible to deliver in-person examinations with proctors or invigilators. For the end of the Winter 2020 semester, and with the support of MacPherson Institute, some instructors transitioned examinations into Avenue to Learn without the use of any additional third-party tools, while other instructors were able to utilize other evaluation methods. And in some cases, marks were determined based on current course standings. These solutions were unlikely to fulfill the needs for all courses, and accredited courses, so a solution to provide a mode for delivering online proctored examinations was prioritized at the end of the winter semester.

To address this challenge, a Steering Committee sponsored by Dr. Kim Dej, Acting-Vice Provost, Faculty, and Ms Gayleen Gray, Assistant Vice President and Chief Technology Officer, was formed to oversee a pilot project and evaluation of online proctoring solutions for Spring/Summer 2020. The larger purpose of this pilot was to evaluate Online Proctoring solutions to recommend a campus-preferred solution for Fall 2020 and what steps might be involved to implement. In addition to the Steering Committee, a project team was formed to undertake the evaluation and pilot online proctoring activities during the spring / summer semester.

Summary

1. A Privacy and Information Security Impact Assessment is conducted when the activity, system, or process is likely to result in imposing risk to the rights and freedoms of students, faculty and/or staff.
2. This process is in compliance with the University's [Information Security Policy](#), [Privacy Governance and Accountability Framework](#), and [Privacy Impact Assessment Protocols](#).
3. This report evidences the University's work to prevent privacy risks to students, and information security risks to the University.

Project Timeline

May 7, 2020	<p>Project Initiation:</p> <p>Working Group formed, and roles defined to assess online proctoring tools for future use as online assessment in University programs.</p>
June 10, 2020	<p>Preliminary Risk Analysis:</p> <p>Preliminary risk analysis conducted on policies and agreements made publicly available. Gaps and discrepancies identified for consultation with vendor.</p> <p>Communications with vendor to request additional details regarding privacy and information security requirements. Project Members to participate in Respondus demonstration of online proctoring service – including exam set-up, learner experience, and assessment functionality.</p>
June 26, 2020	<p>In-depth Risk Analysis:</p> <p>In-depth Risk Analysis based on documentation provided by Respondus, including a Higher Education Community Vendor Assessment Tool (HECVAT).</p>

Analysis

1. Collection of Personal Information: Respondus collects name, address, email, phone number, billing info (where required), photo identification, biometric data via webcam, and data in aggregate to assess trends.
2. Use and Retention of Personal Information: Personal information collected is used for purpose of Respondus' legitimate interest in completing and servicing the financial transaction. Respondus retains personal information via Amazon Web Services (AWS) for a period of 5 years, although licensing institutions can change to alternate period (e.g. 1 year). In addition, licensing institution may request immediate data deletion.
3. Secondary Uses of Personal Information: Respondus does not sell, rent, or otherwise disclose personal information to third parties for their marketing and advertising purposes. However, they may disclose personal information to partner companies where learners have agreed to have that information shared. Respondus attempts to minimize the amount of personal information we disclose to what is directly relevant and necessary to accomplish the specified purpose.
4. Access Control: University instructional staff have sole access to personal information and testing data collected.
5. Privacy and Security Incident Management: In the case of an incident, Respondus' Privacy Centre will notify Respondus Monitor license admin, to provide initial notification to affected individuals within 2 business days of verification, with a more detailed reports sent on a timely basis.
6. Respondus provided a completed Higher Education Cloud Vendor Assessment Toolkit (HECVAT). There were no notable issues arising from the review of the HECVAT.

Key Findings and Recommendations

1. Retention of McMaster student data should be retained by the service provider for 6 months following completion of assessment.
2. The *Graduate Examinations Policy* and *Undergraduate Examinations Policy* should be reviewed to ensure that online proctoring requirements will be compliant.
3. The service provider should provide confirmation of data deletion to the University.
4. Service provider should make menu of accommodations available to the University. This will support minimizing the provision of personal information (e.g. related conditions or other personal health information requiring accommodation). Student Accessibility Services should have the opportunity to identify accommodation requirements to the service provider.
5. Individual students who require accommodation should contact Student Accommodation Services to make formal arrangements.
6. Communication should include direction to test-takers regarding monitor application installation, as part of the online proctoring process. The application must be installed for the duration of the assessment and may be removed/deleted once the assessment is complete.
7. Multi-factor authentication is recommended to enhance access control for students and to provide additional assurance that access to the online proctoring platform is not being abused. Due to the nature of the authentication integration this would require Multi-Factor Authentication to be implemented protecting the Learning Management System (i.e. Avenue to Learn).
8. Where online courses will use online proctoring, the course outline should clearly outline this use to the registered students.

Project Members

Office of the Provost and Vice-President (Academic)

Kimberly Dej	Acting Vice-Provost, Faculty
Kimberly Mason	Academic Integrity Officer

University Technology Services

Gayleen Gray	Assistant Vice President & Chief Technology Officer
Amanda Baldwin	Senior Manager, Strategic Implementations
Paul Muir	Information Security Officer

Paul R. Macpherson Institute for Leadership, Innovation and Excellence in Teaching

Kunal Tandan	Project Manager
Jon Kruithof	Learning Technologies Analyst

Student Accessibility Services, Student Affairs

Allison Drew-Hassling	Director
Mei-Ju Shih	Program Coordinator (Disability Specialist)

Faculty of Business

Randy Walinga	Manager
Alex Biliski	Business Systems Analyst

Privacy Office, University Secretariat

Trudi Wright	Privacy & Records Management Specialist
--------------	---