**Considerations for Use of Third-Party Technologies in Teaching and Learning**

McMaster has a long history of innovative teaching and learning. Today, instructors have access to many digital tools that can help improve the teaching and learning environment. University supported tools are vetted for many factors prior to their procurement, including, but not limited to, data, privacy, security, and other risk factors. However, we recognize instructors may wish to explore third-party technologies that may not be currently supported by the University. Instructors and students should be clear on both the benefits and risks of using third-party technologies before using them for educational purposes.

Following are recommendations to consider prior to implementing third-party technologies in both physical and virtual teaching environments, and to maintaining a respectful and safe learning environment.

If you are considering utilizing an unsupported third-party tool, please consider the following:

**What is a Third-Party Tool?**

A Third-Party tool is a tool that is not officially supported by McMaster University. Some tools are supported centrally, others are supported in Faculties or Departments. Please check with your local IT unit, or email [uts@mcmaster.ca](mailto:uts@mcmaster.ca) to see if the tool you are thinking about using is supported by the University.

**Why do you Need the Tool?**

Ensure that the use of third-party tools has a pedagogical purpose and is in alignment with course learning outcomes. Consider whether the same outcome can be achieved using a University supported tool or through an alternative pedagogical approach.

**Digital Identity:**

Remind all users that anything they post online for a course has the potential to exist indefinitely and that users should conduct themselves online just as they are expected to in a classroom setting. The [Code of Student Rights and Responsibilities](https://secretariat.mcmaster.ca/app/uploads/Code-of-Student-Rights-and-Responsibilities.pdf) continues to apply.

**Informed Consent: Ensure Learners are Aware of What Information may be Collected:**

To inform consent and to ensure transparency regarding the use of personal information, the following steps are recommended:

1. Review the terms of use or end-user license agreement (EULA) particularly regarding the following questions:
2. Is the app allowed to share personal information and with whom?
3. What is the privacy policy?
4. Where is the data stored?
5. Regularly revisit the tool’s privacy settings, as policies change, and platform updates may affect how information is shared.
6. Ensure your course syllabus and your Avenue course shell communicate and outline the use of any third-party technologies as a course expectation.

**Personal Information:**

Avoid contributing data that would be classified as “personal” or “confidential”. If the pedagogical objectives of the course require the instructor or students to enter this type of information, the instructor should not use the tool without consulting with [University Technology Services](https://uts.mcmaster.ca/).

Restrict access to any sensitive information, so that only those with proper permissions can access sensitive information. Do not include any personally identifiable information if avoidable and remove data when it is no longer needed.

**Alternative Option:**

If the instructor wishes to use a third-party tool platform as part of the course curriculum design, instructors should provide students with the choice to “opt out.” Students should not be required to create accounts on non-supported systems or with non-University services.

The course syllabus must specify environments external to the University that are to be used by students as part of course activities. If a student does not consent to participation in an external environment, a viable alternative assignment or activity must be made available to them.

The use of applications that are not supported by the University must follow University guidelines and policies. For example, if there is a cost to use third-party technology, this must adhere to the [Guidelines for Digital Learning Resources policy](https://vpof.mcmaster.ca/app/uploads/2023/02/Guidelines_for_Digital_Learning_Resources-1.pdf).

**Accessibility:**

Third-party technologies, used in teaching and learning should be accessible to all students and be [AODA-compliant](https://www.queensu.ca/accessibility/tutorials/social-media-accessibility) and also meet [WCAG 2.0 AA standards at minimum.](https://www.w3.org/WAI/standards-guidelines/atag/social-media/)

**Intellectual Property:**

The instructor should ensure that use of learning materials incorporated into content uploaded to third-party tools complies with copyright law. Additionally, the instructor should review the terms of service of the third-party tool; typically, the provider claims a license to copy, adapt, and share the content as needed to enable the user to access and use the service. If the license exceeds this limited scope, the instructor should ensure that the owner of the rights (potentially the institution, the instructor, or the student) agrees with these terms.

**Data Privacy and Security:**

Users of the third-party tool should be aware of what data is stored, who has access to the date, how long data is stored and if and how a user can request deletion of their data. Additionally, a user should know if they are able to opt-out of tracking or if their data is being sold to third parties.

Review the security and privacy features of the third-party tool ahead of time, and with students to ensure all are aware of the various settings available.

**Support:**

It is important to recognize that use of a non-University supported tool means there are no dedicated McMaster support services available to users. Any technical support would need to be provided by the vendor. Ensure that you investigate what support services are available to students.

**Additional Support:**

If you would like additional guidance on what you need to consider when using third-party technologies, please reach out to the MacPherson Institute at [mi@mcmaster.ca](mailto:mi@mcmaster.ca) to arrange a consultation.

**Additional Resources**

[McMaster Information Technology Security](https://informationsecurity.mcmaster.ca/people/)

[McMaster Cyber Security Resources](https://cto.mcmaster.ca/it-updates/mcmaster-cyber-security-resources-working-from-home/)

[Guidelines for Social Media Use at McMaster University](https://brand.mcmaster.ca/app/uploads/2019/07/social-media-guidelines.pdf)

[Get Cyber Safe (Government of Canada)](https://www.getcybersafe.gc.ca/en/secure-your-accounts/social-media) – Gov of Canada

[Copyright Office](https://copyright.mcmaster.ca/)