

Guidelines for Use of Non-UW-Madison Applications and Services for Research

Researchers may consider using non-UW-Madison applications and services when conducting their research. While campus-provided applications and services meet UW-Madison guidelines for privacy, intellectual property, security and records retention, providers of non-UW-Madison applications and services may not. This document provides guidance to those researchers considering the use of non-UW-Madison applications and services, as well to those who are already using them.

Terms of Service: Understand the risks to you and your research project.

- Providers of non-UW-Madison applications and services may require the user to agree to a Terms of Service agreement, which is a legal contract. Only a few UW-Madison administrators are authorized to enter into legal contracts on behalf of the UW. Users without that authority become personally responsible for the terms of the agreement and any problems that may arise.
- Providers of non-UW-Madison applications and services may reserve the right to change their Terms of Service at will. Instructors should check the Terms of Service agreement periodically to ensure that the agreement is acceptable.
- UW-Madison has signed agreements for use of some specific non-UW-Madison applications and services and there is no need for you to sign an agreement directly with the provider. Contact policy@cio.wisc.edu for a list of existing campus agreements.
- Contact the Office of Administrative Legal Services at 263-7400 for assistance understanding the conditions and risks associated with using non-UW-Madison applications or services.

Conditions of your grant: Understand the data handling requirements of your grant.

- Check out granting agency requirements for research data handling and storage. It may be that research grant requires research data to be handled and stored on local computers.

Privacy: Protect privacy and identity.

- Restrict access to any sensitive data to researchers.
- Comply with FERPA, HIPAA, and other legal requirements to protect sensitive data.
- Do not place any personally identifiable information if you can avoid it.
- Delete data when no longer needed.
- Safeguard data properly. Researchers failing to do so expose the University and themselves to sanctions and fines. Researchers may also be subject to discipline.

Intellectual Property: Understand who owns content and what they can do with it.

- Review Terms of Service agreement and ask the following questions:
 1. Who owns the intellectual property rights when content is created or uploaded to the application or service?
 2. Does the service provider claim any rights to use the content created or uploaded to the application or service?
 3. If there is a right of use claim, when and how are these rights terminated?
- Identify content as “© 20XX The University of Wisconsin System Board of Regents” when appropriate.
- Encourage researchers to include copyright notices on content if work is to be publicly available.
- Recognize that placing content on a non-UW-Madison application or service may constitute “publication” of intellectual property and may inhibit publication of work through other means and/or prevent patent application.

Retention, Accessibility, Support and Recovery: Comply with regulations and campus policies.

- Ensure that records can be retrieved from the non-UW-Madison application or service provider, if necessary. All UW-Madison business records are subject to public records law, regardless of where they are stored.
- Ensure that university records are retained according to departmentally defined records retention schedule.
- Back up materials residing on non-UW-Madison applications and services regularly. Many providers assume no responsibility for archiving content.
- Consider support needs. Traditional campus support models may not resolve technical issues that arise while using non-UW-Madison applications and services. Users may be required to deal with the service provider directly.
- Ensure non-UW-Madison applications or services meet campus accessibility requirements.

Campus Documents and Policies

- Protecting Your Student Data - http://registrar.wisc.edu/ferpa_overview_fac.htm
- Responsible Use - <http://www.cio.wisc.edu/policies-responsibleuse.aspx>
- Web Accessibility - <http://www.wisc.edu/policies/wwwap.php>
- List of Campus Agreements – contact policy@cio.wisc.edu