Policy Regarding the Use of Non-Approved Information Technology Applications and Hardware for University Business and Instruction

Guidelines

Applications and services, such as online tools, free or paid, that are not owned and operated by UW-Stevens Point might not meet UW-Stevens Point guidelines or requirements for privacy, intellectual property, security, and records retention. Faculty and staff using or considering the use of non UW-Stevens Point or UW System approved applications and services should first seek the approval of the service by contacting Information Technology Purchasing and IT will begin a review. In addition to state level purchasing guidelines, the following factors should be considered when selecting and utilizing applications and services.

Choosing to use Non-University Applications, Technology Tools or Services

Understand the risks to you and others

- Providers may require the user to agree to a Terms of Service agreement. This is a legal contract. Only a few UW-Stevens Point administrators are authorized to enter into legal contracts on behalf of the university. Users without that authority become personally responsible for the terms of the agreement and any problems that may arise.
- Providers may change their Terms of Service without notice. Check periodically to see if it is still acceptable.

Protect sensitive research data and other sensitive information

- Comply with research grant and other contractual and legal requirements to protect sensitive information. There may be requirements that a non UW-Stevens Point application or service cannot meet.
- Restrict access to any sensitive information, so that only those with a “need to know” can access it.
- Do not include any personally identifiable information if you can avoid it.
- Remove data when it is no longer needed.
- The use of any non-approved cloud service for use with High Risk or Moderate Risk data as defined by UW System Administrative policy is strictly prohibited.
- Faculty and staff utilizing tools external to campus-approved tools should not utilize their university password as this is high risk data. Passwords verify identity. It is imperative that users of tools keep their passwords confidential (link to acceptable use document/UWS authentication policy).
- Research of human subjects falls under the definition of High Risk data and may not be placed in non-approved University systems.

Examples of high, moderate, and low risk data

- A complete list of examples can be found at: High Risk or Moderate Risk data as defined by UW System Administrative policy

High Risk	Moderate Risk	Low Risk
Social Security Numbers	Class grades that do not identify the student	“White Pages” directory information
Driver’s License Numbers	Unauthorized for release directory information	Maps, university websites or brochures intended for public use

Financial Account Numbers	Documents or data used internally that have not been authorized for public release	Course catalogs and timetables
Biometrical Numbers (fingerprint, iris image)	Emails or communications not authorized for public release	Student work that does not reflect a grade or student identification numbers
Health Information	Student Campus ID number	
Class grades that identify the student	Data Managed through IRB	
Login info that can access any sensitive info		
Research data		

Protect student privacy

- Comply with FERPA (Family Educational Rights and Privacy Act) requirements to protect student privacy.
- Restrict access to student content whenever possible, so that only those who "need to know" have access.
- Suggest students use aliases when creating accounts, particularly if student work is publicly available.
- Do not place any personally identifiable information in content. Avoid referring to students by full name.
- Limit students' postings to course-related content.
- Obtain student written consent for continued use of student materials beyond the current class.

Communicate the use of non UW-Stevens Point applications and services to students

- Instructors should communicate their intent to use non-UW-Stevens Point applications and services, along with a summary of issues, conditions of use, and risks to students in the course syllabus. Examples of risks include data mining by the company providing the service, selling of student emails to third parties, and ownership of student data shared through the tool. Best practice allows students an 'opt out' provision for use of non-approved university apps and services. An example of a statement that can be included in the syllabus is below:
    - This course requires posting of work online that is viewable only by your classmates. None of the work submitted online will be shared publicly. Some assignments require account creation for online programs. The instructor of this course will not share your academic records (grades, student IDs). Confidentiality of student work is imperative, so you should not share the work of your peers publicly without their permission. By participating in these assignments, you are giving consent to sharing of your work with others in this class and you recognize there is a small risk of your work being shared online beyond the purposes of this course. Examples of additional risks include data mining by the company providing the service, selling of your email to third parties, and release of ownership of data shared through the tool. If you elect to not participate in these online assignments due to confidentiality concerns then an alternate assignment will be offered to you.

Understand who owns content and what they can do with it

- Placing content on a non UW-Stevens Point application or service may constitute "publication" of intellectual property, and may inhibit other publication of the work, or prevent a successful patent application.
- Review the Terms of Service agreement:
    1. Who owns the intellectual property rights when content is created or uploaded to the application or service?
    2. Does the 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?

Consider accessibility, support, retrieval, retention, and backup

- Ensure non UW-Stevens Point applications or services meet campus web accessibility requirements.
- Existing campus support might not resolve technical issues. Users might have to deal with the provider directly.
- Ensure that records can be retrieved from the provider. UW-Stevens Point records are subject to public records law.
- Ensure that university records are retained according to records retention schedules.
- Back up material regularly. Many providers assume no responsibility for backing up content.

Choosing to use Non-University hardware

- Employees conducting university business which involves high risk data as defined by UW System policy are required to perform that work on a University approved device or through a university secured network. Moderate or high risk data should not be stored on personally owned devices. Devices found to be in violation of this policy will be blocked from the University network. All devices and paid software to conduct University business as specified are to be purchased through IT Purchasing with University funds. This includes, but is not limited to; computers, laptops, mobile devices, tablets, phones, and printers. If you have a question, about this policy please contact IT Purchasing. Personnel who do not abide by this requirement may be asked to return the product/cancel service and may lose purchasing card privileges.
- Non-approved hardware does not possess the same warranty terms as approved University hardware and will be subject to hourly repair rates from Information Technology in the event service is required.
- Users may access university email and Office 365 services using personal devices. This provides users convenience with access to critical data services. The use of one's own device should not be a primary method for conducting University business or in lieu of a provisioned IT device. When used on campus, personal devices will be required to connect to the University domain and have data managed through that domain. In addition, data stored on those devices is subject to any open records or legal requests made of the University and the device will need to be provided to IT security for review in the case of such a request.

References

- UW System Administrative Information Technology Policies
- UW System Policies
- Wisconsin Public Records Law Management
- Human Subject Research Guidelines UW – Stevens Point