PRIVACY IMPACT ASSESSMENT (Short-Form)

See Guidance for Completion of Privacy Impact Assessments for detail about each of the below questions.

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Wrike Project Management
Organization:	University of the Fraser Valley
Business or Academic Unit	Marketing
Initiative Lead name and title:	Laura Authier
Initiative Lead phone:	
Initiative Lead email:	laura.authier@ufv.ca
Privacy Officer:	Stephen Gaspar
Privacy Officer phone:	Ext. 4654
Privacy Officer email:	Stephen.gaspar@ufv.ca

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
No
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.

No
Related PIAs, if any:
n/a

1. What is the initiative?

The Marketing team is looking to deploy a cloud-based project management solution, Wrike, that does the following:

- PMO management with features that keep strategy, planning, and execution aligned.
- 360° visibility, with automation, and one-click reporting.
- Capability to balance workloads, optimize resources, and drive productivity with all-in-one resource management.
- Ability to monitor project performance with instant analytics and visualize progress through multiple views — ideal for Agile, Waterfall, and more.
- No coding or complex configuration required. Navigate the intuitive interface with ease, lean on ready-to-go templates.
- Customize workflows, fields, and views, and use Custom Item Types to reflect your best practices.

2. What is the scope of the PIA?

The entire initiative to configure and utilize Wrike Project Management by the VP, Community Engagement division at the University of the Fraser Valley is covered by this PIA.

3. What are the data or information elements involved in your initiative?

Please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative.

Consider segmenting your response into the different categories of people who you will collect different types of information from (e.g. students, administrators, employees, alumni, etc.).

Please include where the information is coming from (directly from users, pulled from pre-existing UFV databases, etc.)

User type	Data Elements/Category	Data Source
Faculty	Not anticipated to be collected.	n/a
Staff	Contact Information: First Name, Last Name, email address, office number	UFV AD Global Address List
Administrators	Contact Information: First Name, Last Name, email address, office number	UFV AD Global Address List
Names and emails of external partners and contractors to UFV	Contact Information: First Name, Last Name, email address, address	Through communication with external partners and contractors, individuals may be invited to collaborate on a project with UFV staff. UFV staff will be able to invite these individuals by entering it into Wrike. This information is anticipated in most cases to be contact information, rather than personal information.
Students, alumni, donors	Not anticipated to be collected. However, it is possible that if a student is involved in a project (as an interview subject or a spokesperson) that their name, email address or phone number	

	may be included within a project file.	

3.1 Did you list personal information in question 3?

***Personal information* is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.**

Yes.

It is expected that in project management cases, contact information will be stored in the system. Other personal information is not anticipated to be required to be stored.

4. How will you reduce the risk of unintentionally collecting personal information?

Wrike project management software will be used to manage project tasks, timelines, collaboration, and communication among team members. To address the potential risk of unintentionally collecting personal information during the use of the software and how to mitigate that risk the following controls will be applied:

The project management software may collect some contact information such as names, email addresses, and phone numbers of team members. It is important to note that this information is necessary for effective project management, and therefore, it is reasonable to collect and process it. However, Wrike and the team will not collect any unnecessary personal information or other sensitive data, which are not relevant to the project management process.

There is a risk of unintentionally collecting personal information in project management software if the system is not properly configured or if the user lacks awareness of privacy settings. This risk can arise when team members share personal information in project tasks, discussions, or files, which are not relevant to the project management process.

Wrike will be configured to only collect essential personal information required for project management purposes.

All team members will be provided with training on how to use the software's settings and encouraged to adhere to the University's privacy practices. Also, the system will be monitored to ensure that it is not collecting any unnecessary personal information.

By taking these steps, Wrike will be able to effectively manage projects while maintaining privacy.

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using, and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use and disclosure.

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FOIPPA authority**	**Other legal authority**
Contact information may be used to identify an individual as part of the normal activity in project management. This contact information may be included when a project is opened or may be added as the individual is assigned to a project, or is responsible for an activity.	Collection, Use	Section 26(c), Section 27 and 27 (3) Section 32(a)	
Wrike is a cloud-based solution and project information will be stored in its data centers as part of the solution.	Disclosure	Section33(2)(d), Section 33(2)(t)	

6. Collection Notice

If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

Personal information will not be collected directly from individuals for this initiative. To the extent contact information will be used to identify an individual, such information will have already been collected by UFV and sourced from the Active Directory Global Address List (GAL), or for individuals who are contractors, or otherwise external to UFV, from the individual themselves under the authority of section 26(c) of FIPPA.

PART 3: STORING PERSONAL INFORMATION

If UFV is storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

- Yes

8. Does your initiative involve sensitive personal information?

- No

9. Where are you storing the personal information involved in your initiative?

s. 15(1)(l), s. 17, s. 21 [redacted]. While data may be saved at other locations, all facilities are certified and covered by Wrike's Privacy Policy:

https://www.wrike.com/security/privacy/

This policy also includes Wrike's policy on data transfers between its California site and other international data centres. This includes Wrike's adherence to the European Union-US Privacy Shield framework which covers the collection, use and retention of personal data.

PART 4: SECURITY OF PERSONAL INFORMATION

In Part 4 you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

10. Does your initiative involve digital tools, databases or information systems?

- Yes

11. If the answer to question 10 is "yes", has UFV's IT Security Office completed a security assessment.

Wrike has provided a HECVAT (Higher Education Cloud Vendor Assessment Toolkit) which has been reviewed by UFV's IT Security Office and determined to meet all relevant requirements.

12. Has UFV's Privacy Protection Schedule and/or Cloud Security Schedule been attached to the Contract?

    - No

PART 5: ACCURACY, CORRECTION AND RETENTION

In Part 5 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

13. How will UFV make sure that the personal information is accurate and complete?

In general, personal information collected will be limited to contact information necessary for effective project management. Generally, this contact information will be specific to the team itself, and should not include other employee, faculty or student data. If personal information is collected directly by the project team under the authority of section 26(c) or indirectly, any inaccuracy will be corrected upon request of the individual.

14. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

1.1 Do you have a process in place to correct personal information?

-Yes

If personal contact information collected is inaccurate it will be corrected upon request of the individual.

15. Does your initiative use personal information to make decisions that directly affect an individual?

-No

16. Do you have an information schedule in place related to personal information used to make a decision?

FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision.

-No

Part 6: ADDITIONAL RISKS

17. Has the vendor expressed, either through contract, communications with you, or their privacy policy, their agreement to notify UFV of a privacy breach?

-Yes

Wrike has committed through its Information Security Addendum (https://www.wrike.com/legal/enterprise-winfosec/) to notify customers as follows as part of its Incident Response:

> *Wrike will inform Customer of a confirmed security incident within the time period required by law. Wrike will notify Customer at the email address associated with Customer's administrator account, or at another email address that Customer provides to Wrike in writing for purposes of security incident notifications.*

18. Risk Response (non-security risks)

Describe any additional risks that arise from collecting, using, storing, accessing, or disclosing personal information in your initiative that have not been addressed by the questions on the template.

If you filled in the risk table at Q.14 for sensitive information stored outside of Canada, only include additional risks here.

Add new rows if necessary.

Possible (non-security) risk	Proportionate response / mitigation strategies
The vendor uses third party subcontractors that they do not agree to be accountable for related to privacy practices.	Contractual language

PART 7: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

None.

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer / Privacy Office Representative			

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Electronic signature	Date signed
Initiative lead			
Contact Responsible for Systems Maintenance and/or Cyber Security.	Crawford Millen		