PRIVACY IMPACT ASSESSMENT (PIA)
CLOSURE SUMMARY

Initiative	ThoughtFarmer Intranet Platform
PIA Reference #	2025-004
PIA Completion Date	May 9, 2025
Project Sponsor	April van Ert – Vice-President, Brand, Communication and Engagement
Unit	BCE

The purpose of a PIA is to determine whether an initiative complies with the *Freedom of Information and Protection of Privacy Act* ("**FIPPA**") and JIBC's policies and procedures. This document confirms that the PIA review of this initiative has been completed. The following outlines the scope, issues, legal basis and conclusions associated with this PIA.

Initiative Description & Scope

ThoughtFarmer is a cloud-based intranet platform that will serve as a centralized hub for internal communications, resource sharing, and employee engagement. The system supports functions such as news posting, team pages, organizational announcements, and document sharing. The platform will be used exclusively for internal purposes and does not involve the collection of new or sensitive personal information.

Information Reviewed

Our review is based on the completed PIA Questionnaire (attached as Schedule A), with additional consultation provided by Technology Services. Technology Services has confirmed that, from a technical perspective, the platform meets reasonable security standards required under section 30 of FIPPA. No vendor access to personal information is anticipated.

Legal Basis - Privacy

While the platform does not collect new or sensitive personal information, section 27(2) of FIPPA requires that individuals be informed about the collection of any personal information. Accordingly, a simple collection notice should be included during onboarding or posted in a prominent section of the intranet. An example of such a notice is included at the back of this document.

The platform will involve limited processing of personal information, primarily consisting of employment-related data (e.g., name, position, business contact information, and staff photos). This use of personal information is authorized under section 26(c) of FIPPA, as it relates directly to and is necessary for a program or activity of the public body — specifically, internal communications and organizational coordination.

The information is classified as "Confidential", but does not include medical, financial, or other high-risk personal information. Accordingly, it is not considered sensitive for the purpose of section 33.1 of FIPPA and does not trigger supplementary risk assessment requirements.

Pursuant to section 32(a) of FIPPA, a public body may use personal information in its custody or under its control for the purpose for which the information was obtained, or compiled, or for a use consistent with that purpose.

Pursuant to section 33(2)(d) of FIPPA, a public body may disclose personal information for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose. Pursuant to section 34 of FIPPA, a use or disclosure of personal information is consistent with the purpose for which the information was obtained or compiled if the use: (a) has a reasonable and direct connection to that purpose; and (b) is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses or discloses the information.

JIBC does not anticipate using the platform to make decisions that directly affect individuals, but if such functionality evolves, compliance with the following will be required:

- Section 28 – JIBC must make reasonable efforts to ensure the personal information is accurate and complete before using it for such decisions.
- Section 31 – JIBC must retain the personal information for at least one year after it is used in such a decision to allow the individual to access it.

Legal Basis - Security

Pursuant to section 30 of FIPPA, JIBC must ensure personal information is protected by reasonable security arrangements against unauthorized access, collection, use, disclosure, or disposal. Based on confirmation from Technology Services, the ThoughtFarmer platform has been reviewed and deemed satisfactory in this regard. No access from outside of Canada is expected, and no transmission of personal information to third parties is involved.

The data will be stored within Canada and access is restricted to JIBC users via secure login. No integration with student or sensitive HR systems is contemplated at this time.

Conclusions

Based on the information provided, the ThoughtFarmer platform may be used for its intended purpose, provided that:

- A compliant collection notice is incorporated (e.g., via onboarding, posted notice on the intranet, or a simple pop up at the first visit to the intranet)
- Access is appropriately role-based and limited to internal users
- Any material changes to the system's use or the nature of personal information processed trigger a renewed PIA review

Responsibilities

BCE should ensure that employees are informed about the collection and use of personal information through the platform. A sample collection notice could be:

"Your personal information is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act. This information is used for internal communication and employee engagement purposes within JIBC. If you have any questions about the collection of this information, please contact privacy@jibc.ca."

BCE is also responsible for notifying the General Counsel of any significant changes to the platform's use or to the types of personal information processed, as such changes may require a renewed PIA review.

If you have any questions or concerns about this PIA, please contact the General Counsel.

SCHEDULE A
PIA QUESTIONNAIRE

Please see attached.

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

for

ThoughtFarmer

1. Purpose of the Privacy Impact Assessment Questionnaire

This form is used by JIBC to provide a high-level overview of the potential privacy risks of a current or proposed policy, system, project, program or activity. The results of these screening questions help judge the level of potential risk, the extent to which risk mitigation strategies may be needed and when completion of a privacy impact assessment is required under the *Freedom of Information and Protection of Privacy Act* (British Columbia) (the "**Act**").

2. Privacy Questions

Questions	Answers
Does the program involve personally identifiable information (PII) (as defined by the Act)? [Y/N]	Y
Will the program involve the collection or creation of new information about individuals? [Y/N]	N
Will personal information about individuals be disclosed to organizations, programs, processes or people who have not previously had routine access to the information? [Y/N]	N
Will personal information about individuals be used for a purpose it is not currently used for, or in a way it is not currently used? [Y/N]	N
Will the program require contacting individuals in ways that they may find intrusive? [Y/N]	N
Does the program have a collection notice or use policy? [Y/N]	N

3. Technology Questions

Questions	Answers
Does this program involve the implementation of a new electronic system or use of a new application or software to support the creation, collection, updating or storing, backing-up or disposition of personal information? [Y/N]	N
Does this program require any modifications to existing information technology (IT) systems (e.g., integration with or consolidation of other IT systems)? [Y/N]	N
Will a new or modified electronic system change the existing business workflow? [Y/N]	N
Does the program involve the use of new technology that might be perceived as being privacy intrusive? [Y/N]	N

4. Impact Questions

Questions	Answers
What are the purpose of collection, use and/or disclosure of the personal information? [Internal/External/Both]	Internal
Will personal information about the same individual that was previously maintained separately now be aggregated and stored together? [Y/N]	N
How would you describe the information classification level of the personal information? (Select all that apply) • Highly Confidential • Confidential • Public	Confidential
What are the type(s) of personal information? (Select all that apply) • Bio/demographic information • Academic/education Information • Employment information • Medical/health Information • Financial Information • Criminal information • Images • Opinions about individuals • Individuals' personal views and opinions • Business contact information • Personal contact information • Other	Bio/demographic information Employment information Images Business contact information
What are the type(s) of individuals? (Select all that apply) • Prospects • Applicants • Students • Employees • Donors/alumni/other 3rd parties • Volunteers • Service providers • Other	Employees Volunteers

How many records documenting individuals will be stored, accessed, used or disclosed? [1-1000], [1001-5000], [5,001-50,000], [50,001-100,000], [100,000+]	1-1000
How many JIBC employees, volunteers and service provider employees will be able to access, collect, use or disclose the information? [1-10], [11-50], [51-100], [101-250], [251-500], [501-1,000], [1,000+]	251-500
Is any of the information owned by another organization? [Y/N]	N

5. Probability Questions

Questions	**Answers**
Where will the information be stored? (Select all that apply) • On campus – JIBC servers • On campus – other • Off-campus – inside Canada • Off-campus – outside Canada	Off-campus – inside Canada
Is any of the information accessed from outside of Canada? [Y/N]	
Will personal information be transmitted? (Select only one) • Personal information is used in a closed system (i.e., no connections to the Internet, Intranet or any other system and the circulation of hardcopy documents is controlled) • Personal information is used in a system that has connections to at least one other system • Personal information is transferred to a portable device (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed • Personal information is transmitted using wireless technologies	• Personal information is used in a system that has connections to at least one other system
Will a third party (e.g., vendor or service provider) have access to the information? [Y/N]	N
Will the program result in different record keeping systems converging? [Y/N]	N