BCNET 30 Years
Shared Services for Higher Education & Research

Privacy Impact Assessment

Ellucian Ethos

Table of Contents

Note to BCNET Member Institutions:

This Privacy Impact Assessment (PIA) has been created for the benefit of Member Institutions. Member Institutions should customize the contents of this PIA to ensure it accurately reflects their use of the system or program being assessed. Areas highlighted in red are for information only and should be deleted or replaced with the Member Institution's information.

PART 1: GENERAL INFORMATION

Initiative title:	Ellucian Ethos
Organization:	BCNET
Branch or unit:	Shared Systems and Technologies
Your name and title:	Jo-Ann Bellamy Hooper Access and Privacy Consulting Ltd.

Your work phone:	250-208-3431
Your email:	jbellamy@hooperconsulting.ca
Initiative Lead name and title:	Dean Crawford Director, Shared Systems and Technologies BCNET
Initiative Lead phone:	250-721-8477
Initiative Lead email:	dean.crawford@bc.net
Privacy Officer:	Bev Hooper Hooper Access and Privacy Consulting Ltd.
Privacy Officer phone:	250-896-4272
Privacy Officer email:	bev@hooperconsulting.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:
A PIA has been completed by BCNET for Amazon Web Services (AWS). A PIA has been completed by BCNET for Ellucian Banner Cloud. <Member institutions should list any related PIAs they have completed.>

1. What is the initiative?

BCNET is a federally incorporated not-for profit services and information technology organization that represents the interests of its member institutions comprised of 25 publicly funded universities, colleges, institutes, and research organizations across British Columbia. It represents all public, post-secondary education institutions in the province and provides shared services to its members in the areas of networks, procurements, licensing, and IT services.

BCNET completed a Privacy Impact Assessment on the Ellucian Ethos platform on behalf of its member institutions in 2019. This PIA is being completed to update any information which may have changed since the completion of the original PIA.

Ellucian Ethos is a higher education platform that connects people, processes and applications across the institution to power coordinated programs designed for student success. Ethos is a single data model that powers all APIs and integrations across the institution's technology and application footprint. This allows for end-to-end workflows and a single source of truth for analytics; providing the data to make better informed decisions.

The average campus ecosystem includes dozens of applications serving a particular business need while also adding to the integration complexities that IT teams face each day. Ethos was developed as an open platform to drive down total cost of integration ownership and maintenance. Ellucian invites partners to move away from custom integrations to a packaged approach so that we may all serve the higher education community better. By becoming Ethos connected, individual application data can be combined with other campus data to enable institutions to act and engage with the community.

Ellucian Ethos features include:

- APIs and integrations - Connect applications and speed up implementation with standard APIs and integrations.
- Institutional data sharing - Reduce maintenance by replacing brittle point-to-point integrations with robust integrations.
- Cloud-based data repository - Provides a consolidated source of institutional data for sophisticated operational and analytical reporting needs.
- Management console - Gives the ability to manage and monitor enterprise integrations.
- Identity management- Create seamless, secure accessibility, and maximize security through rigorous ID management and ensure compliance.

The Ellucian Ethos system works in cooperation with other Ellucian applications (e.g., Banner, Colleague, etc.) and partners through a cloud-based hub for exchanging data.

Ellucian Ethos is hosted by Amazon Web Services in Montreal. A connected system can reside on premises, in the cloud or in a hybrid model, and all connect to the same unifying Ethos integration platform.

The Ellucian Ethos platform is available to all BCNET members who are Ellucian licensees.

2. What is the scope of the PIA?

This PIA addresses the collection, use, disclosure, storage, access, and security of personal information in the Ellucian Ethos platform.

BCNET has completed a PIA for AWS (Canada).

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

<Member institutions should ensure the information elements listed below are accurate and complete for their use of Ellucian Ethos.>

Examples of information elements include:

- Name
- Contact information, e.g., email, address, phone number
- Date of birth
- Gender
- Financial information
- Education history
- Work history
- Medical information

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.

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template.

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

N/A

PART 2: COLLECTION, USE AND DISCLOSURE

5. Collection, use and disclosure

<Member Institutions may customize the table below to ensure it accurately reflects their collection, use and disclosure of personal information.>

Ellucian Ethos provides two distinct methods for users:

- **API - under this model an integrated system can request data from Ellucian Ethos at any time and will wait for the response to be returned from the authoritative application (e.g., CRM Recruit).**
- **Subscription - under this model an integrated system will periodically check for changes in the authoritative system (Banner/Colleague) and update information in systems accordingly.**

API:

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**
Step 1: Personal information is initially collected from individuals.	Collection	26(c)	
Step 2: User securely logs in to an integrated system (CRM Recruit) to obtain information (e.g., to generate a unique student recruitment mailing list for a specific marketing campaign).	Use	26(c)	
Step 3: Integrated system requests data from Ellucian Ethos, which in turn routes the request to CRM Recruit to populate remaining info.	Use Disclosure	32(a) 33(1) and (2)	
Step 4: CRM Recruit provides additional info (in accordance with security models (implemented/managed at the institutional level).	Use	32(a)	
Step 5: Ellucian Ethos returns the info to the requesting system and data is automatically removed from Ellucian Ethos (no data is stored).	Use Disclosure	32(a) 33(1) and (2)	

Subscription:

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**
Step 1: An individual record (e.g., student, employee) is updated in Banner or Colleague.	Collection	26(c)	
Step 2: A change notification is created and published by Banner or Colleague to Ellucian Ethos.	Use Disclosure	32(a) 33(1) and (2)	
Step 3: Ellucian Ethos queues the message to subscribers (a subscriber is a system that is notified of changes via Banner/Colleague).	Use Disclosure	32(a) 33(1) and (2)	

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
Step 4: Subscribing systems retrieve the change notification and process the info update. Once all subscribers have retrieved the data it is removed from Ellucian Ethos (no data is stored).	Use Disclosure	32(a) 33(1) and (2)	

6. Collection Notice

<Member Institutions are responsible for ensuring the appropriate notification is in place prior to the collection of personal information.>

PART 3: STORING PERSONAL INFORMATION

7. Is any personal information stored outside of Canada?

No.

8. Does your initiative involve sensitive personal information?

Yes.

- If yes, go to question 9
- If no, go to question 10

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No.

- If yes, go to question 10
- If no, go to Part 4

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

After you answer this question go to Part 5.

N/A

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada.

11. Is the sensitive personal information stored by a service provider?

N/A

- If yes, fill in the table below (add more rows if necessary) and go to question 13

- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
N/A		

12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

N/A

13. Does the contract you rely on include privacy-related terms?

N/A

- If yes, describe the contractual measures related to your initiative.

14. What controls are in place to prevent unauthorized access to sensitive personal information?

N/A

15. Provide details about how you will track access to sensitive personal information.

N/A

16. Describe the privacy risks for disclosure outside of Canada.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.
N/A					

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

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

Yes

17.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?

No

- If yes, you may want to append the security assessment to this PIA. Go to question 19
- If no, go to question 18

18. What technical and physical security do you have in place to protect personal information?

<Member Institutions are responsible for ensuring the technical security of all data in their custody and/or control (including data at rest or in transit) and must meet applicable technical security standards required by their organization.>

Ellucian

The Ellucian Ethos platform is hosted on AWS (Canada). For more information on AWS Data Center controls, see the BCNET PIA on AWS (Canada) or https://aws.amazon.com/compliance/data-center/controls/

Ellucian aligns itself with industry best practices and complies with key standards and regulations. Ellucian's information security program is modeled on the ISO 27001 Information Security Management System framework, and Ellucian is compliant or aligns with several international industry security standards and regulations for cloud platform solutions.

Each year, an independent audit firm conducts Ellucian's annual Service Organization Control (SOC) audits. The SOC1 and SOC2 Type II reports are available to customers for review upon request and execution of a non-disclosure agreement. The SOC3 report is available at https://www.ellucian.com/assets/en/ellucian-soc3-report-2021-22.pdf

Ellucian Cloud Services achieved its ISO27001:2013 certification in 2021. The certificate is available at https://www.ellucian.com/assets/en/ellucian-iso27001-certificate.pdf

See Appendix A for additional information on Ellucian Cloud security.

19. Controlling and tracking access

<Member institutions are responsible for controlling and tracking access to information for their organizations.>

Strategy	
We only allow employees in certain roles access to information	Yes or No
Employees that need standing or recurring access to personal information must be approved by executive lead	Yes or No
We use audit logs to see who accesses a file and when	Yes or No
Describe any additional controls:	

PART 6: ACCURACY, CORRECTION AND RETENTION

20. How will you make sure that the personal information is accurate and complete?

<Member Institutions are responsible for ensuring personal information is accurate and complete.>

Updates to an individual's information is recorded in one of the integrated systems (e.g., Banner, Colleague, etc.) by a Student, Faculty or Staff. Ellucian Ethos automatically retrieves the change notification and processes the update for all integrated systems.

21. 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.

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

Yes.

<Member Institutions are responsible for ensuring a process is in place to correct personal information.>

Ellucian

Ellucian Ethos does not store personal information. Correction of personal information is the responsibility of the member institution.

21.2 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

<Type "yes" or "no" to indicate your response. Member Institutions are responsible for ensuring a process is in place to document the request to correct or annotate the record.>

21.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

<Type "yes" or "no" to indicate your response. Member Institutions are responsible for notifying other public bodies or third parties of the request for correction.>

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

No.

- If yes, go to question 23
- If no, skip ahead to Part 7

23. 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. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule.

N/A

- If no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

PART 7: AGREEMENTS AND INFORMATION BANKS

24. Does your initiative involve an information sharing agreement?

No.

25. Will your initiative result in a personal information bank?

No. Records are not retained in Ellucian Ethos beyond integration events.

PART 8: ADDITIONAL RISKS

26. Risk response

Note: Primary responsibility for the management and administration of any physical and or technical security risks is born by member institutions when using Ellucian Ethos.

Possible risk	Response
Risk 1: Unauthorized individuals at member institution could access personal information.	<Member institution is responsible for security of personal information, e.g., Employee code of conduct, confidentiality agreements, privacy training and awareness, privacy policies, access controls, strong passwords, least privilege and need-to-know principles, monitoring, etc.>
Risk 2: Unauthorized individuals at Ellucian could access personal information.	Ellucian utilizes a combination of online and offline security technologies, procedures, and organizational measures to help safeguard Personal Data. For example, facility security is designed to prevent unauthorized access to Ellucian computers. Electronic security measures — including, for example, network access controls, passwords, and access logging — provide protection from hacking and other unauthorized access. Ellucian also protects Personal Data through the use of firewalls, role-based restrictions and, where appropriate, encryption technology. Ellucian limits access to Personal Data to employees, subcontractors, and third-party agents that have a specific business reason for accessing such Personal Data. Individuals who have been granted access to Personal Data will be made aware of their responsibilities to protect such information and will be provided training and instruction on how to do so.
Risk 3: Ellucian's use of third-party service providers (e.g., member institution is utilizing a third-party tool such as TouchNet)	Ellucian shares Personal Data with subcontractors, business partners and third-party agents and contractors only to the extent required to deliver products or services requested by customers. Before

Possible risk	Response
	transferring Personal Data to these third parties, Ellucian will obtain assurances from the recipient that it will safeguard Personal Data in a manner consistent with Ellucian's Privacy Notice and otherwise to support Ellucian business activities.
Risk 4: User's personal information is compromised during transmission	Ellucian maintains a strong encryption standard, aligned with industry standards, that governs use of encryption technology in Ellucian Cloud Solutions offerings and across the company. These encryption methods are regularly evaluated to address and remediate changes to their effectiveness or security. Advanced application data encryption is also available to Ellucian customers, allowing for the encryption of sensitive application data completely transparent to the application. Available encryption methods are application dependent.
Risk 5: Security breach at Ellucian	Ellucian has a detailed incident response plan in place in the event of a security incident, and 24x7 monitoring of its security systems and alerts.

PART 9: 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

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	Bev Hooper Hooper Access and Privacy Consulting Ltd.		April 12/23

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
Head of public body, or designate Only required if personal information is involved	Dean Crawford Director, Shared Systems and Technology	Dean Crawford	17 April, 2023