Privacy Impact Assessment

Moodle

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

PIA file number: BCNET_Moodle PIA_April 2023

Initiative title:	Moodle PIA
Organization:	BCNET
Branch or unit:	

Your name and title:	Megan Jacobson, Hooper Access and Privacy Consulting Ltd.
Your work phone:	236-464-1105
Your email:	mjacobson@hooperconsulting.ca
Initiative Lead name and title:	Devon Keys
Initiative Lead phone:	
Initiative Lead email:	devon.keys@bc.net
Privacy Officer:	Bev Hooper
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:
BCNET has completed a PIA on their internal EduCloud platform. <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.

Moodle is a learning platform designed to provide educators, administrators, and learners with a single, secure, and integrated system to create personalized learning environments. It is an open-source software system that is deployed by a multitude of educational and corporate

organizations to deliver course content while minimizing service costs. Moodle also provides enhanced flexibility and functionality for higher education institutions and is considered a leader in electronic course deliver with over 90 million users worldwide.

BCNET has proactively led the implementation of the Moodle software application on behalf of its members. The Moodle environment was originally transitioned from BCcampus to BCNET in 2016. The production service is currently hosted by BCNET in British Columbia and is available to the eligible BCNET members. Moodle is deployed in a secure environment that provisions reliable EduCloud server infrastructure and network connectivity.

A shared Moodle service minimizes the cost and effort required to provide the functionality and support for electronic service delivery. It assists institutions in taking advantage of opportunities for increased collaboration by providing an environment with a consistent approach to patching, plugins, and configuration. Moodle is housed in a secure, highly available environment, including the provision of a reliable server infrastructure, network connectivity and MySQL/PostgreSQL and Moodle patching and upgrades patching. The core product is used by students, faculty, and staff.

A key component of facilitating innovative information technology (IT) solutions through this advanced network is ensuring they are hosted, accessed, managed, and protected within a secure environment in accordance with Provincial (Freedom of Information and Protection of Privacy Act, FIPPA) privacy laws, regulations, and controls.

BCNET is committed to ensuring that the use of Moodle meets provincial privacy and security legislative requirements, policies, and practices, and works with its members to strive to reduce the privacy risks associated with the legislative requirements accordingly. These privacy risks are managed through a combination of technical, administrative, and physical controls that mitigate the associated risk. This privacy impact assessment (PIA) is intended to allow BCNET and its members who wish to utilize applications such as Moodle to proceed and to ensure that these services are offered and provided in a way that is compliant with the Freedom of Information and Protection of Privacy Act (FIPPA).

2. What is the scope of the PIA?

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

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 the system or program.>

The following information elements may be collected and processed when using Moodle through a Member Institution's account:

Student:

- Username
- Password

- First Name
- Last Name
- Primary Email
- Student ID
- Course
- Grades
- Video/Audio assignment footage
- Work assignments
- PI disclosed while using the 'Chat' functionality

Employee/Faculty (for workplace training only):

- Username
- Password
- First Name
- Last Name
- Primary Email
- Employee ID
- Training Course
- Grades

System Administrators:

- Username
- Password

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.>

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: BCNET members (IT) login to Moodle with credentials using Single Sign On, LDAP authentication or Moodle Authentication.	Collection	26(c)	N/A
Step 2: Authorized 'People Profiles' are created with the appropriate assigned permissions (can be also implemented via student information systems such as Banner).	Use	32(a)	N/A
Step 3: Users are given permissions to Moodle as appropriate by an IT Administrator (regularly reviewed). Users log in using secure credentials & work in the modules for which they have been assigned permission.	Use	32(a)	N/A
Step 4: Discontinued user data is exported and deleted from Moodle by BCNET members (IT) upon termination of the contract between Moodle and client.	Use	32(a)	N/A

See Appendix A.

6. Collection Notice

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

(INSTITUTION) is committed to ensuring that the personal information you provide is protected. The personal information that you provide is collected under the authority of (COLLEGE AND INSTITUTE ACT or UNIVERSITY ACT) in accordance with the Freedom of Information and Protection of Privacy Act, section 26(c). Your personal information will be used for the following (PROVIDE ALL USES). For questions regarding the collection, disclosure, and security of your personal information, please contact (NAME and EMAIL ADDRESS). >

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?

N/A

- After you answer this question go to Part 5.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

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

<**Note to Member Institutions:** Moodle is hosted within BCNET's EduCloud within 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)?

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					

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?

BCNET Member Institutions

<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.>

As the primary repository for course content is developed by participating BCNET members, robust and regular backup procedures are highly recommended to ensure complete control.

EduCloud

Using the VMWare NSX solution, the operations team can configure security rules for individual VDCs. With NSX, the operations team can lock down application, create a logical DMZ in software, and reduce the attack of a virtual desktop environment. NSX Data Center enables micro-segmentation to define and enforce network security policies consistently on any workload hosted anywhere. All features are configurable and administered by the member administrators with support provided by the EduCloud operations team as required.

EduCloud – Physical Security

EduCloud is hosted on secure servers in two geographic locations (Vancouver and Kamloops) within B.C. Data centers protected by access controls. Access is continuously monitored both electronically and by cameras. Only authorized personnel have access to the secure data centers.

EduCloud – Technical Security

Data at rest: BCNET and member data is hosted in EduCloud. All user information is stored in a Microsoft SQL Server database. All database files are stored on encrypted disks using 256-bit AES encryption block cipher. Database backups are encrypted as part of the backup process using 256-bit AES encryption block cipher.

Multi-factor authentication. Environments (production, non-production, etc.) are on segregated networks and have separate database servers, web servers, load balancers, etc. This ensures that deployments to a lower environment cannot target production systems.

EduCloud Disaster Recovery
At present there is no Disaster Recovery (DR) plan or service option in place for Moodle. However, EduCloud automatically creates backups that are stored both locally and remotely at the other data center as part of the service. In the event of a disaster recovery, prioritization will be dependent on site/EduCloud instance and internal priorities.

SIEM and CrowdStrike
Security Information and Event Management (SIEM) is in operation with all Moodle VM servers within BCNET's SIEM. The SIEM looks for suspicious activity and monitors for tax on the servers. SIEM casts a wide net to catch nefarious activity. CloudStrike cybersecurity, though it casts a smaller net, is a real-time tool that acts on immediate attacks. Cloudstrike monitors all Moodle endpoints and uses automated threat intelligence protection and remediation should its analytics tool see an attack on the servers.

Thompson Rivers University/Sonicat
BCNET provides operational support only to its subscribed members (e.g. Server upgrades, new plug-ins, new version upgrades, database maintenance & backups) of the Moodle service.

BCNET and its members can work with Thompson Rivers University (TRU) technical support staff to manage and resolve all incidents and issues raised and reported. TRU contracts with a third party (Sonicat), to provide Moodle Tier 2/3 support. All TRU technical support staff are located in BC and third party service providers are located in Ontario (within Canada). BCNET members have sole control and responsibility of the information they share with technical staff as permitted under Section 33.1 of the Act.

https://www.tru.ca/its/infosecurity/standards/Information_Security_Policies.html
https://www.tru.ca/its/infosecurity/standards.html

Thompson Rivers University/Sonicat – Physical Security
Support staff access the Moodle virtual machines (VM) remotely through EduCloud. They are responsible for ensuring the physical security of all data while in their custody and/or control (including data at rest and in transit) and must meet all applicable security standards as required by BCNET.

Thompson Rivers University/Sonicat – Technical Security
Support staff are responsible for ensuring the technical security of all data while in their custody and/or control (including data at rest and in transit) and must meet all applicable security standards as required by BCNET.

Support staff access Moodle VMs through the EduCloud administrator panel as well as through command line SSH. SSH utilizes “public key cryptography” to authenticate connections in order to prevent unauthorized access. Access logs are maintained and periodically reviewed.

Moodle

https://docs.moodle.org/36/en/Category:Security
https://docs.moodle.org/36/en/MoodleDocs:Privacy

Moodle is hosted in the EduCloud environment. EduCloud is hosted on secure servers in two geographic locations (Vancouver and Kamloops) within B.C. Data backups are located in Vancouver and Kamloops respectively. The platform is restricted to authorized user and not by geographic location. All personal information stored by member will reside on servers within Canada.

Moodle – Physical Security

Moodle is an open-source software platform independently deployed by BCNET for its members (governed by the EduCloud PIA security measures & principles). Vendor contact does not occur. where the digital records for your initiative are stored (e.g., on your organization’s LAN, on your computer desktop, etc.) and the technical security measures in place to protect those records. Technical security measures include secure passwords, encryption, firewalls, etc. Physical security measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc.

Moodle – Technical Security

Moodle is an open-source software platform independently deployed by BCNET for its members (governed by the EduCloud PIA security measures & principles). Vendor contact does not occur.

19. Controlling and tracking access

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

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:	BCNET: BCNET, its members and their service providers are solely responsible for the strict management and

Strategy	
	administration of user access based on need to know including the maintenance and enforcement. EduCloud: EduCloud operators cannot access or alter personal information in any way. Thompson Rivers University/Sonicat: Support staff do not access or alter personal information in any way unless specifically requested to do so by an institution's designated Moodle Administrator in extenuating circumstances. BCNET members subscribed to the Moodle service can work with support staff to manage and resolve all incidents and issues raised and reported. Members have access to technical support staff during regular business hours, as outlined in the Service Level Agreement between BCNET and the service operator. BCNET members have control and responsibility of the information they share with technical staff when they contact them at the time as permitted under Section 33.1 of the Act. Moodle: Moodle does not have access to the personal information that resides within the system.

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.>

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?

<Type "yes" or "no" to indicate your response. Member Institutions are responsible for ensuring a process is in place to correct personal information.>

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?

Yes, BCNET members control and may use personal information to make a decision that directly affects an individual in the course of using the system when administering programs and services.

- 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.

<Type "yes" or "no" to indicate your response. BCNET member institutions are responsible for having an information schedule in place.>

- 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?

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

Yes.

Describe the type of information in the bank
Registration through Moodle includes all personal information as outlined in #3 (above).
Name of main organization involved
BCNET
Any other ministries, agencies, public bodies or organizations involved
Used by authorized BCNET staff, BCNET members, students, and PSI staff in support of implementation and deployment of the Moodle system.
Business contact title and phone number for person responsible for managing the PIB
<If "yes", BCNET member institutions are responsible to complete.>

PART 8: ADDITIONAL RISKS

26. Risk response

Possible risk	**Response**
Risk 1: Unauthorized individuals at BCNET or member institutions could access personal information and use or disclose it for personal purposes.	Employee Code of conduct and Non-disclosure agreements, Use of Information & Technology Policies, staff training, password protected access, user access to system, based on need-to-know principles, permission restrictions, access controls, and monitoring.
Risk 2: User's personal information is compromised during transmission from member institution to Moodle.	Encrypted by Moodle during transfer of data (HTTPS, SSL TLS 1.2, AES 128/256 cipher suites).
Risk 3: Moodle (EduCloud) security breach	Moodle & EduCloud employ robust security standards, policies, staff training, breach strategies and remediation protocols. EduCloud is FIPPA compliant.
Risk 4: Unauthorized individuals at Thompson Rivers University/Sonicat could access personal information and use or disclose it for personal purposes.	Employee Code of conduct and Non-disclosure agreements, Use of Information & Technology Policies, staff training, password protected access, user access to system, based on need-to-know principles, permission restrictions, access controls, and monitoring.

PART 9: SIGNATURES

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	Dean Crawford	Dean Crawford	2023-07-07

Appendix A

Personal Information Flow Diagram