BCNET 30 Years
Shared Services for Higher Education & Research

# Privacy Impact Assessment - Moodle

| | | | |
|---|---|---|---|
| Name of Organization | BCNET | | |
| PIA Drafter: | Hooper Access and Privacy Consulting Ltd. (Tracy Jo Reid) | | |
| Email: | bev@hooperconsulting.ca<br>tjreid@hooperconsulting.ca | Phone: | 250 896-4272<br>250 388-0145 |
| Program Manager: | Dean Crawford | | |
| Email: | Dean.crawford@bc.net | Phone: | 250 721-8477 |

## 1. Description of the Initiative

BCNET is taking the lead on the development of this Privacy Impact Assessment (PIA) of Moodle on behalf of its members and affiliations.

BCNET is a federally incorporated not-for profit, services information technology organization that represents the interests of its members (including 25 publicly funded post secondary institutions) made up of universities, colleges, institutes, and research institutes 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.

This unique and collaborative shared services model provides a multitude of benefits to its members from reducing and containing costs and increasing spending power, to decreasing duplication and improving service quality and productivity. The model cultivates a strong community, where members actively engage with peers to share, explore and develop innovative ideas and solutions as they tackle a broad spectrum of common and unique research and education technology challenges and topics. BCNET strives to add value to its membership by leveraging an advanced network that provides economies of scale to maximize efficiencies and drive down collective costs, while at the same time, continuing to facilitate collaborative innovative solutions that meet the needs of their stakeholders in support of world-class research and education.

As government, education and public-sector organizations face unique challenges to accomplish complex mandates with limited resources, they are overwhelmingly turning to the power and speed of technology and infrastructure to serve citizens more effectively, achieve scientific breakthroughs, and educate students.

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. Scope of this PIA

This PIA has been developed with a focus on the privacy protection and security measures deployed by Moodle in the Canadian cloud environment. This includes use of Moodle by BCNET members, its services and operational controls as it relates to Privacy, Security and Data Protection in British Columbia.

This PIA does not speak to the contractual requirements and responsibilities of BCNET and its members in meeting their privacy obligations when entering into service agreements for Moodle.

## 3. Related Privacy Impact Assessments

A PIA has been completed on the EduCloud platform by BCNET.

## 4. Elements of Information or Data

Student:

User Name
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):

User Name
Password
First Name
Last Name
Primary Email
Employee ID
Training Course
Grades

System Administrators:

User Name
Password

## 5. Storage or Access outside Canada

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

Disaster Recovery:

At present there is no Disaster Recovery (DR) plan or service option in place for Moodle. However, EduCloud automatically creates backups as part of the service. A full EduCloud High Availability (HA) service using Zerto for VM replication is currently being implemented for the Moodle Service. In the event of a disaster recovery, prioritization will be dependent on site/EduCloud instance and internal priorities.

BCNET member support:

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.

**6. Data-linking Initiative***

| **In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.** | |
|---|---|
| 1. Personal information from one database is linked or combined with personal information from another database; | No |
| 2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled; | N/A |
| 3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies. | N/A |
| **If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.** | |

**7. Common or Integrated Program or Activity***

| **In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.** | |
|---|---|
| 1. This initiative involves a program or activity that provides a service (or services); | Yes |
| 2. Those services are provided through:<br>(a) a public body and at least one other public body or agency working collaboratively to provide that service; or<br>(b) one public body working on behalf of one or more other public bodies or agencies; | No |
| 3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation. | N/A |
| **Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.** | |

## 8. Personal Information Flow Diagram and/or Personal Information Flow Table

See *Appendix A* – attached.

| Personal Information Flow Table | | | |
|---|---|---|---|
| | **Description/Purpose** | **Type** | **FOIPPA Authority** |
| **1.** | BCNET members (IT) login to Moodle with credentials using Single Sign On, LDAP authentication or Moodle Authentication. | Collection | *26(c)* |
| **2.** | 'People Profiles' are created with the appropriate assigned permissions (can be also imported via student information systems such as Banner). | Use | *32(a)* |
| **3.** | Users are given permissions to Moodle as appropriate by an IT Administrator (regularly reviewed). Users login using secure credentials & work in the modules for which they have been assigned permission. | Use | *32(a)* |
| **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)* |

## 9. Risk Mitigation Table

| Risk Mitigation Table | | | | |
|---|---|---|---|---|
| | **Risk** | **Mitigation Strategy** | **Likelihood** | **Impact** |
| **1.** | Unauthorized individuals could access the personal information in the system and use or disclose it for personal purposes. (within the Moodle environment – EduCloud) | Employee Code of conduct and non-disclosure agreements; password-protected access, user access based on need to know, permission restrictions, role based access controls, multi-factor authentication, privacy training and audit/monitoring. | Low | High |
| **2.** | BCNET/member personal information data is compromised during transmission from the BCNET/member to Moodle | Encrypted by Moodle during transfer of data (HTTPS, SSL TLS 1.2, AES 128/256 cipher suites). | Low | High |
| **3.** | Moodle (EduCloud) security breach | Moodle & EduCloud employ robust security standards, policies, staff training, breach strategies and remediation protocols. EduCloud is FIPPA compliant. | Low | High |

## 10. Collection Notice

BCNET and its members are responsible for ensuring the appropriate collection notification (for the specific application/program) is in place prior to the collection of personal information and before transmission to Moodle.

## 11. Please describe the physical security measures related to the initiative (if applicable).

**BCNET:**

BCNET, its members and their service providers 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 the applicable physical security standards required by their organization.

**EduCloud:**

The EduCloud service is hosted in two secure 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.

**Thompson Rivers University/Sonicat:**

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.

**Moodle:**

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.

## 12. Please describe the technical security measures related to the initiative (if applicable).

**BCNET:**

BCNET, its members and their service providers 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 physical 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:**

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.

**Thompson Rivers University/Sonicat:**

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:**

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.

**13. Does your branch/department rely on any security policies?**

**BCNET:**

BCNET, its members and their service providers are responsible for the deployment, dissemination and administration of all organizational security policies etc. as it relates to the handling and management of personal information in their custody and/or control.

**EduCloud:**

Using the VMWare NSX solution, members can configure security rules for their individual VDC. With NSX, members have the ability to 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 configured and administered by the member with support provided by the EduCloud operators as required.

**Thompson Rivers University/Sonicat:**

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

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

**Moodle:**

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

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

**14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.**

**BCNET:**

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

**15. Please describe how you track who has access to the personal information.**

**BCNET:**

BCNET, its members and their service providers are responsible for ensuring that access to all personal information in their custody and/or control is controlled, monitored and reviewed/audited on a regular basis.

**EduCloud:**

EduCloud operators do not have access to BCNET member personal data unless required under Section 33.1 of the Act.

**Thompson Rivers University/Sonicat:**

Support staff do not have access to BCNET member personal data unless required under Section 33.1 of the Act.

**Moodle:**

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

16. **How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?**

    Responsibility for ensuring all personal information is up to date and accurate lies with BCNET and its members.

17. **Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.**

    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.

18. **If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

    Responsibility for ensuring all personal information is up to date and accurate lies solely with BCNET members who have subscribed to the service.

19. **If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?**

    Responsibility for records retention and/or disposition schedules lies solely with BCNET members.

20. **Does the initiative involve systematic disclosures of personal information? If yes, please explain.**

    No.

21. **Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.**

    No.

22. **Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.**

    Yes.

    a. Moodle system.
    b. Registration through Moodle includes all personal information as outlined in point 4. above.
    c. Section 26(c)
    d. Obtained, compiled and used for the implementation and deployment of the Moodle system.
    e. Used by authorized BCNET staff, BCNET members, students and PSI staff in support of implementation and deployment of the Moodle/system.

**Signed on Behalf of BCNET:**

Dean Crawford

Dean Crawford
Director, Shared Systems and Technology
BCNET

2019-07-24
Date

Digitally signed by Bala Kathiresan
DN: cn=Bala Kathiresan, o=BCNET, ou=President and CEO, email=bala.kathiresan@bc.net, c=CA
Date: 2019.07.24 17:21:51 -07'00'

Bala Kathiresan
President and Chief Executive Officer
BCNET

July 24, 2019
Date

*Appendix A*

**BCNET**
**Privacy Impact Assessment - Moodle**
**Personal Information Flow Diagram**