BCNET

Privacy Impact Assessment
D2L Brightspace LMS & AWS

Part 1 – General

Name of Department/Branch:	BCNET		
PIA Drafter:	Hooper Access and Privacy Consulting Ltd. (Roseann Whitton)		
Email:	rwhitton@hooperconsulting.ca bev@hooperconsulting.ca	Phone:	250-920-6331 250-896-4272
Program Manager:	Dean Crawford/Devon Keys		
Email:	dean.crawford@bc.net devon.keys@bc.net		250-721-8477 250-721-7635

1. Description of the Initiative

BCNET is taking the lead on the development of this Privacy Impact Assessment (PIA) on behalf of its members and affiliations who are using the D2L Brightspace Learning Management System (LMS) platform. It also incorporates the impact of D2L's recent move in selecting Amazon Web Services (AWS) as it's public cloud infrastructure service provider.

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 services.

This unique, 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.

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*, FOIPPA) privacy laws, regulations and controls.

D2L's Brightspace (Brightspace) is a digital learning management platform that is currently deployed by BCNET member institutions in delivering personalized learning experiences in a classroom or online to people anywhere in the world. Brightspace is cloud-based, and offers multimedia to increase engagement, productivity and knowledge retention. The platform makes it easy to design courses, create content, and grade assignments, giving instructors more time to focus on teaching and learning. It is used for both face-to-face and distance education, and supports the learning experience through course content management, student assessment, collaboration, and course communications. It is BCNET members' specific roles and rights-based systems in which a range of user types are created and access to information is granted to users based on the operational needs of their role. This access is strictly managed and controlled by each individual BCNET member institution. At the same time, BCNET members can utilize analytic reports that track and deliver insights into the performance levels of departments, courses, or individuals.

To use Brightspace, information from the BCNET member's Enterprise Resource Planning and Student Information System (ERP) (e.g. Banner) must be transferred to Brightspace. The ERP is the foundational system that collects and stores all data related to students, faculty, staff and courses. This complex system delivers a full range of functions from strategic management to records processing. In addition, the ERP enables the deployment of essential integrated systems and applications that are required to support major workflows necessary to operate and manage the business. Each BCNET member is currently responsible for storing their own personal information held in their ERP.

BCNET members currently use third party integration brokers of their choosing (e.g. Message Broker) specific to their institution to move the data securely from their ERP's into D2L's Brightspace. The information that is transferred is limited to what is required to use the tools in the Brightspace learning management system. Updates made in BCNET member institution ERPs (e.g. student enrollments, course drops, faculty enrollments, course changes, etc.) are sent by the integration broker to Brightspace over SSL in real time.

Previously the data in D2L's Brightspace was hosted internally in D2L data centres located in Waterloo, Ontario (primary) and Calgary, Alberta (secondary), and was stored and accessed within Canada. In selecting AWS Canada region as its' cloud infrastructure service provider, services previously hosted on D2L internal servers in Canada will now be hosted on AWS servers located in AWS Canadian region, ensuring the data continues to reside within Canada. In selecting AWS as its cloud service provider, D2L supports and accelerates its innovation by leveraging built-in AWS services such as Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), Amazon CloudFront, Amazon Elasticsearch, and the suite of AWS analytics and security services. AWS's reliability, security, and availability allows D2L to continue to provide a high level of service and end-to-end security on a trusted global infrastructure to BCNET members.

2. Scope of this PIA

This PIA covers the collection, use and disclosure of personal information from BCNET member ERP's to the D2L Brightspace LMS platform as well as covers the changes of the host system from D2L to AWS cloud servers. Personal information previously hosted in D2L's internal data centres will now be hosted in the AWS Canada region. This PIA is intended to cover the services, and operational controls in place for both D2L and AWS as it relates to Privacy, Security, and Data protection in British Columbia.

This PIA does not speak specifically to the contractual requirements and responsibilities of BCNET members in meeting their privacy obligations when entering into their service agreements with D2L.

However, is should be noted that all member contract agreements with D2L must include language that covers and speaks to the protection of personal information in accordance with the *Freedom of Information and Protection of Privacy Act* (FIPPA) and as a best practice, include a Privacy Protection Schedule.

3. Related Privacy Impact Assessments

No other PIA's have been completed on D2L on behalf of BCNET, however one was done for the British Columbia Institute of Technology (BCIT) on their specified use of the product. In addition, a comprehensive PIA has been completed by BCNET on AWS. The AWS PIA covers the full spectrum of their services and their operational controls and measures (to include disaster recovery) deployed in the Canadian Cloud environment to identify and assess potential vulnerabilities to BCNET members and the community at large.

4. Elements of Information or Data

The collection of all personal information into the ERP will continue to be the responsibility of each individual BCNET member. In this context, the personal information (PI) is the PI that is securely transferred directly from the BCNET member's ERP into the D2L Brightspace LMS now hosted in AWS servers. (**note:** AWS offers D2L strong encryption for content in transit or at rest, including the option to manage their own encryption keys).

The BCNET member is responsible for the secure transmission of the data from their operating system into D2L Brightspace LMS.

Standard data elements required for D2L Brightspace LMS include (i.e. from student, faculty or staff):

- Full Name
- Organizational defined ID/Username (user's ERP ID/password)
- E-mail address
- Course registration
- In-course activity (discussion posts, e-mails, uploads, exams, grades, etc.)
- IP address (logged) for each system access

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

D2L:
D2L is a Canadian company that hosts its Brightspace LMS system in AWS data centres in Canada. Data is not stored or accessed outside of AWS servers in Canada. D2L manages the data in accordance with the *Personal Information Protection Act* (PIPA) of British Columbia and Canadian privacy regulations and control the access keys to the data. At no time does AWS have direct access to data that is being processed unless it is necessary in response to a D2L client request.

D2L retains control of this content and it is their responsibility to manage their data backup plans. AWS does provide backup services, but D2L has the option of arranging independent back-up services from an alternative service provider for additional protection if they so choose.

AWS:
Please refer to the AWS PIA for further detailed information related to this section.

Under the above noted circumstances, all data transmitted between the BCNET member ERP, D2L and AWS is within Canada only.

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;	Yes
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
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: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (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

BCNET members that have deployed the Brightspace LMS assume responsibility and management of their ERP operating system (including updates and security patches), other associated application software, configuration of the D2L provided security group firewalls, and other security, change management, and logging features. Example of the flow of information between the BCNET member ERP and D2L.

Flow Table – ERP to D2L Brightspace LMS:

The ERP is the primary control for access to D2L. Although it may vary from institution to institution, there are typically three variations on how data is exchanged:

Note:
For clarity, the process has also been described generally from the end user/member experience, although actual member experience may vary slightly.

1. Term Setup
   - Completed three times per year just before registration is turned on for the coming term
   - An extract of the ERP data is completed by the BCNET member and sent (encrypted using secure transmission) to D2L Brightspace.
   - D2L Brightspace imports this data to setup the new term.
   - This process is for setting up course instances and attaching existing instructors to them.

2. Ongoing Live Integration
    - Once the term is setup, registration is opened for the coming term and "live integration" is turned on.

Section 15(1)(l)

For example:

- New account creations – personal information data
- Registration – course assignment data

3. Logins
    - Once the above has occurred, users can login to D2L Brightspace through the ERP login process.
    - Personal information will be securely processed while in the ERP. Section 21, Section 15(1)(l)

As a web-based application, Brightspace uses a range of dynamic web pages to present and collect data. The following is an example of a user experience and how the data flows behind the scenes:

1. User logs into the system with their user ID and password.
2. The system looks up the user's role at the ERP Org Level which at this point is the level all users first access upon login before going to a course.
3. Based on their role, the dynamic nature of the page presents them with the information and functional tools they are entitled to at that level, such as:
    - News showing just the messages targeted to students
    - Personal tools and settings
    - My Courses listing
    - My Calendar

    At this level, there is little personal information and none about other users for any role except System Administrators.
4. Users may then access a secondary Org Level based on their role. The system checks the user's role at the new level (a course for example) and delivers the web page configured with the tools and features appropriate to their role and associated rights. Depending on their role, they may or may not have access to personal information, for example:
    a. A System Administrator may access Admin Tools, then Users, conduct a search for a specific user, and then Edit User seeing the following:
        - Username (ERP ID)
        - Org Defined ID (ERP ID)
        - First Name
        - Last Name
        - E-Mail
        - User enrolments

- Login history – date, time and IP address

b. A Student logging into a course would see the following (depending on course settings):

- Their own name
- Any additional personal information they had chosen to add to their profile
- First and last names of those in this class
- Any class discussion posting from those in this class (or could be restricted to just the Group they are in)

c. An Instructor/Designer going to a new course under development may see:

- First and last name of the others (usually Designers as well) in this course
- Org Defined ID (ERP ID) for others in this course
- E-mail address for others in this course
- Last access date and time

d. An Instructor going to a current course would see:

- First and last name of others in this course
- Org Defined ID (ERP ID) for others in this course
- E-mail address for others in this course
- Last access date and time
- Discussion postings from others in this course
- Exam submissions for students in this course
- Assignment submissions for student in this course
- Gradebook log for students in this course
- Access logs for student including date, time and IP address
- Activity logs for student showing time spent on in-course activities

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	Students register in the BCNET member ERP.	Collection	26(c)
2.	Faculty are assigned courses in the ERP.	Collection	26(c)
3.	Brightspace LMS collects personal information for use in courses from the ERP through the BCNET member specific integration broker.	Use	32(a)
4.	Member students and faculty access Brightspace via a secure connection using their ID and password.	Use	32(a)
5.	Authentication is performed by the BCNET member specific single sign-on log-in system.	Use	32(a)
6.	Students' assignments, work products and exams are submitted through and stored in Brightspace.	Use	32(a)
7.	Faculty grade assignments and exams in Brightspace.	Use	32(a)
8.	Student updates made in the ERP are sent over in real-time or through a nightly batch transfer to Brightspace via a secure connection.	Use	32(a)

D2L Brightspace LMS to AWS:

In using AWS cloud infrastructure for cloud computing/applications, the security and compliance responsibilities are shared between D2L and AWS. D2L controls how they architect and secure the Brightspace application and the data put on the infrastructure, while AWS is responsible for providing services on a highly secure and controlled platform and providing a wide array of additional security features.

D2L

(Responsible for Security "IN" The Cloud)

CUSTOMER DATA - BRIGHTSPACE LMS
PLATFORM, APPLICATIONS IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)

D2L: *A*ssumes responsibility and management of the guest operating system (including updates and security patches), other associated application software, configuration of the BCNET member cloud-provided security firewalls, and other security, change management, and logging features.

AWS

(Responsible for Security "OF" The Cloud)

COMPUTE STORAGE DATABSE NETWORKING

AWS Infrastructure: REGIONS/AVAILABILITY ZONES/EDGE LOCATIONS

AWS Canada: operates, manages, and controls the infrastructure components, from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

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 BCNET)	Employee Code of conduct and Non-disclosure agreements; Use of Information & Technology Policies, password protected access, user access to system, based on need to know basis, permission restrictions, controls, and monitoring.	Low	High
2.	Personal information is compromised when transmitted into D2L.	Section 15(1)(l)	Low	High
3.	Unauthorized individuals could access the personal information in the system and use or disclose it for personal purposes (within D2L)	Contractual privacy protection flow downs between BCNET member and D2L. D2L internal security and privacy standards.	Low	High
4.	D2L Security Breach	D2L breach protocols are in place to reduce risks to client data in the event of a security breach.	Low	High
5.	Personal information data is compromised during transmission from D2L to AWS.	Section 15(1)(l)	Low	High
6.	AWS Cloud Security Breach	AWS breach protocols are in place to reduce risks to client data in the event of a security breach.	Low	High

10. Collection Notice

The BCNET member is responsible for ensuring the appropriate collection notification (for the specific application/program) is in place prior to the collection of all personal information into their ERP and before transmission to D2L.

Part 3 – Security of Personal Information

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

BCNET:
BCNET members are responsible at all times for ensuring the physical security of all data while in their custody and/or control (including all data at rest or in transit) and must meet all applicable physical security standards required by their organization. Although they may vary from institution to institution it typically includes the following: data centres are secured in locked facilities, security key access cards are provided only to authorized staff, access logs are kept and monitored, CCTV and physical security patrols.

D2L:

Section 21, Section 15(1)(l)

AWS:

Please refer to the AWS PIA for further detailed information related to this section.

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

BCNET:

BCNET members are responsible at all times for ensuring the technical security of all data while in their custody and/or control (including all data at rest or in transit) and must meet all applicable technical security standards required by their organization. Although they may vary from institution to institution it typically includes: Data in the ERP is stored in a database located behind corporate firewalls that block all connections to the database from the internet. The integration broker is used as an intermediary between D2L and the data. Access to this server is restricted via an access control list on the Load Balancer (e.g. NetScaler). When information is ready for delivery to D2L it is sent through an SSL connection.

D2L:

Section 21, Section 15(1)(l)

Section 21, Section 15(1)(l)

AWS:
Please refer to the AWS PIA for further detailed information related to this section.

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

BCNET:
BCNET members 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. Although they may vary from institution to institution, they typically include the following standard policies:

- Acceptable Use of Information Technology
- Information Security
- Safety, Security and Emergency Management

D2L:
D2L is responsible for the deployment, dissemination and administration of their own internal organizational security policies etc. as it relates to the handling and management of personal information in their custody and/or control as well as those required under contract by the BCNET member.

- Security Policies & Protection https://www.d2l.com/security/policies/
- Privacy Statement https://www.d2l.com/legal/privacy/

AWS:
Please refer to the AWS PIA for further detailed information related to this section.

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 members are responsible for the strict management and administration of user access based on a "need to know" basis only, including maintenance and enforcement.

Students have unique user IDs and passwords and self-manage changes. Students who wish to make changes through their institution's Registrar typically are required to show identification. Access to the system by faculty and staff is granted based on individual roles and responsibilities.

The course owner is the person responsible for the course and authorized to grant access to others.

D2L:

Section 21, Section 15(1)(l)

AWS:
Cannot access or alter personal information in any way.

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

BCNET:
BCNET 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.

D2L:
A previously noted above, access is provided based on user needs at each of the different levels of D2L and within each of the different course shells that a user has authorization to access. In cases where a student enrols in a course, the ERP provides student level access to that course automatically. In a case where the same student withdraws from a course, the ERP removes access to that course in D2L.

In cases where user access is provided manually, D2L assess need and duration and will, where appropriate, remove access to a course environment. Once a user has access to the BCNET member Org Level, the highest level in D2L, that access is never removed. It should be noted that this is also the level that provides the least access to PI or any information about others in the system.

AWS:

AWS does not have access to D2L (BCNET member) personal data unless required under Sections 17 or 18 of the *Personal Information Protection Act* (PIPA). Please refer to the AWS PIA for further detailed information related to this section.

Part 4 – Accuracy/Correction/Retention of Personal Information

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?

The BCNET member ERP is the authoritative source for all user data in D2L. Approved changes made in the ERP automatically populate to D2L's Brightspace LMS in real time or nightly batch transfer.

Under no circumstances do D2L or AWS alter personal information in any way.

(**Note:** Designated members of D2L do have access to BCNET members Brightspace site for support related troubleshooting. D2L is ISO 27001 (information management security) and ISO 27018 (protection of personally identifiable information) certified. D2L has its own Security Management System of policies, procedures, and controls based on the ISO 27001 control framework, following ISO 27002 control best practices where applicable.)

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

Yes, personal student work products are reviewed and graded in Brightspace. Marks and feedback are retained in Brightspace and final course grades are typically manually entered into the BCNET member ERP. Should a student fail a course, the individual assignment and test marks are also logged into the ERP.

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.

Each BCNET member's faculty are responsible for the accuracy and completeness of the information.

19. If you answered "yes" to question 17, do you have 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?

Each member institution is responsible for their Records Management retention schedule and related policies.

Part 5 – Further Information

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) Name: Student Course Information – D2L
Address: BCNET member specific address.

(b) Student personal information includes: first and last name, organization defined ID/Username, e-mail address, course registration, in-course activity, exam results and grades, and IP address

(c) Information is collected under the authority of the *College and Institute Act,* RSBC, 1996, c. 52 and section 26 of the *Freedom of Information and Protection of Privacy Act* RSBC, 1996, c. 165

(d) Information is collected, used and disclosed only for purposes directly related to and needed by BCNET members to assess students' eligibility for admission, enrolment, decisions on academic status, graduation, record keeping, statistical research or program evaluation, and other purposes consistent with member mandate; the administration and operation of member programs and services pursuant to the *College and Institute Act;* students being members of the BCNET member specific community and attending a public post-secondary institution in the Province of British Columbia including the programs of the BCNET member specific Student Association, BCNET member specific Alumni Association, and the BCNET member specific Foundation; and as required by provincial and federal government authorities or authorized by law.

(e) Access to information is based on roles and responsibilities assigned to BCNET member specific employees.

Part 6 – Sign Off
BCNET Director

Dean Crawford　　23 September 2020

Dean Crawford
Director, Shared Systems & Technology
BCNET

Date

Head of BCNET

Bala Kathiresan
Bala Kathiresan (Oct 9, 2020 08:11 EDT)　　Oct 9, 2020

Bala Kathiresan
President & Chief Executive Officer
BCNET

Date

A final copy of this PIA (with all signatures) must be kept on record.