Privacy Impact Assessment for Non-Ministry Public Bodies

BlackBoard - J&B Learning – Navigate2 Curriculum- Fire and Safety Division

JIBC PIA# - 2014.003

Why do I need to do a PIA?

Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA. Public bodies should contact the privacy office(r) for their public body to determine internal policies for review and sign-off of the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.

If you have any questions about this PIA template or FOIPPA generally, you may contact the Office of the Chief Information Officer (OCIO) at the Privacy and Access Helpline (250 356-1851). Please see our PIA Guidelines for question-specific guidance on completing a PIA.

What if my initiative does not include personal information?

Public bodies still need to complete Part 1 of the PIA and submit it along with the signatures pages to their privacy office(r) even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

Part 1 – General

Name of Department/Branch:	School of Public Safety – Fire and Safety Division		
PIA Drafter:	**Luc Lang**		
Email:	llang@jibc.ca	Phone:	**604.528.5791**
Program Manager:	**Mika Fryling**		
Email:	mfryling@jibc.ca	Phone:	**604.528.5668**

In the following questions, delete the descriptive text and replace it with your own.

1. Description of the Initiative

The initiative coincides with the launch of a new Fire Fighting Technologies Certificate. Some curriculum, content, access and authorization will be hosted by J&B Learning. The purpose of this initiative is to offer standard content from a Learning Technologies vendor, using existing in-house BlackBoard Learning Management System (LMS) tools. Three J&B learning content cartridges called Navigate 2 will be delivered to the JIBC for use in three courses that are offered in the certificate program. Content is compliant with the latest National Fire Protection Association (NFPA) standards and meets Canadian requirements. Although assessments are part of the

Navigate 2 offering, quizzes will be administered via JIBC's local BlackBoard LMS, and an in-house installation of QuestionMark will be used to administer final exams in the 3 courses.

2. Scope of this PIA

The scope of the PIA covers access to materials delivered both through a cloud solution from J&B Learning via JIBC's local BlackBoard LMS or through the installation of local cartridges installed on JIBC servers and accessed via a local installation of BlackBoard. All information, both public and personal will be stored in Canada regardless of the solution. This PIA covers all phases of delivery of on-line content. Assessment (quizzes and examinations) are out of scope of this initiative and will be conducted internally via existing local JIBC assessment/exam technology (QuestionMark).

3. Related Privacy Impact Assessments

There are no additional PIAs relating to this initiative.

4. Elements of Information or Data

Elements of data that form part of the service offered by J&B Learning via JIBC's local installation of BlackBoard include: User ID, Course ID, Assessment ID and Assessment Scores (if assessment quizzes) are used. Assessments, including quizzes and examinations will be administered internally either via Blackboard, or an on-premise installation of QuestionMark exam administration software.

Please refer to attached data flow diagram in **Exhibit 1** and revised **Exhibit 7** which excludes BlackBoard Partner Cloud solutions.

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

S.15(1)(l)

5. Storage or Access outside Canada

[redacted]

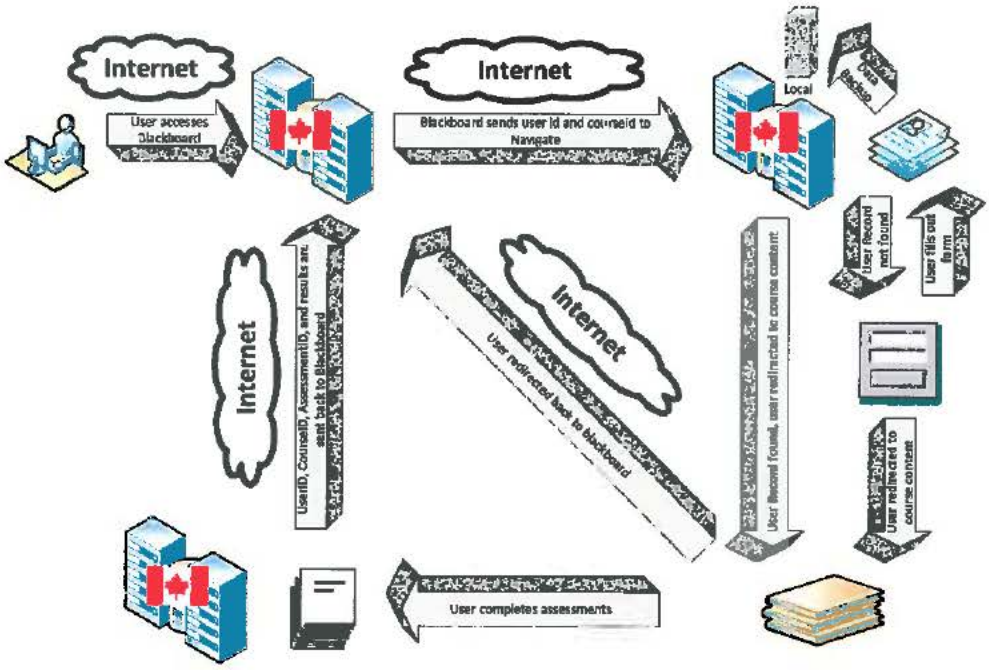
6. Data-linking Initiative*

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/no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	yes/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.	yes/no
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/no
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;	yes/no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	yes/no
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



*Note: Although the above diagram shows data flow for assessments, assessments will be conducted in-house via on-premise exam administration software.

Please refer to **Exhibit 1** and **Exhibit 7** at end of PIA

9. Risk Mitigation Table

Examples can be removed and additional lines added as needed.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Employees could access personal information and use or disclose it for personal purposes*	*Employees hired by J&B Learning go through a background check before they are hired.*	*Low*	*High*
2.	*Student's information is compromised by unauthorized access to storage facility*	*Physical security is in place where information will be stored, if stored on J&B architecture, in Canada*	*Low*	*High*
3.	*Student's personal information is compromised when transferred to the service provider*	*Transmission is encrypted and over a secure socket layer (SSL)*	*Low*	*High*
4.	*Student's information is accessed by external intrusion*	*Student's information is protected by firewall technology both at the JIBC and at J&B Learning in Canada*	*Low*	*Medium*

10. Collection Notice

Collection notice is given to students via the JIBC Privacy notice located here:

http://www.jibc.ca/privacy

Privacy notice included as **Exhibit 3** at end of PIA

Part 3 – Security of Personal Information

If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with your public body's privacy office(r) and/or security personnel when filling out this section. They will also be able to tell you whether you will need to complete a separate security assessment for this initiative.

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

[redacted] S.15(1)(l)

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

[redacted]

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

Yes, JIBC Information Security Policy **Exhibit 4** and JIBC Information and Educational Technology Acceptable Use policy **Exhibit 5**

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.

[redacted]

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

Access to student personal information is tracked through Training Partner, a Geometrix product that is currently used as JIBC's Student Information System. Access to student data is tracked and controlled by employee function and by Schools. The Registrar's Office has overall responsibility to

maintain student's personal information. Some personal information maintenance such as ID and password information by System e.g., JIBC's LMS are delegated to an LMS system administrator. In most cases where personal information is changed, an audit of the change is tracked by User ID.

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?**

    Users have access to update their own information. Personal information can also be updated by authorized JIBC staff.

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

    Yes, assessment scores (quizzes and examinations) are used to determine a grade for the student when above curriculum is offered. Control, access and authorization continue to be administered locally.

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.**

    Assessments will be done via QuestionMark, a secure product that is administered by JIBC staff in-house.

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?**

    Yes, the JIBC has a retention policy, attached as **Exhibit 6** at the end of this document.

Part 5 – Further Information

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

The initiative does not involve systematic disclosures beyond an established exchange of information with the Ministry of Education in the provincial Central Data Warehouse (CDW).

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).	

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

The initiative does not involve access to personally identifiable information for research and statistical purposes beyond those required by the Ministry of Education for their Central Data Warehouse or information mandated to be provided to Statistics Canada.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).	

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.

A personal information bank (PIB) will not result from this initiative.

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the Privacy Office(r) as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to Privacy Office(r).

Privacy Officer/Privacy Office Representative	Signature	Date
Peter Kingston	Peter R. Kingston	9/18/2014

Privacy Impact Assessment for Non-Ministry Public Bodies

BlackBoard - J&B Learning – Navigate2 Curriculum- Fire and Safety Division

JIBC PIA# - 2014.003

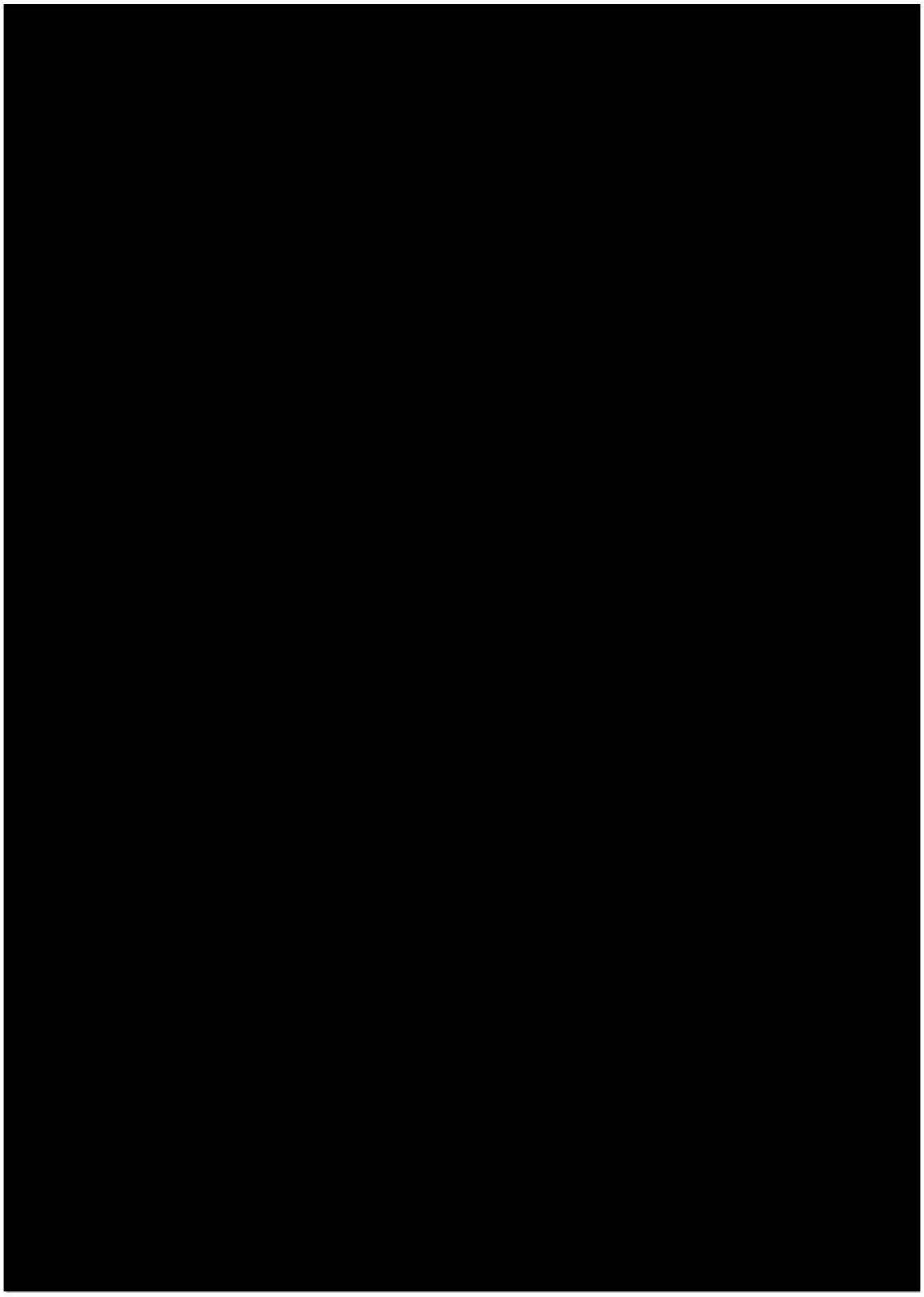
Part 7 – Program Area Signatures

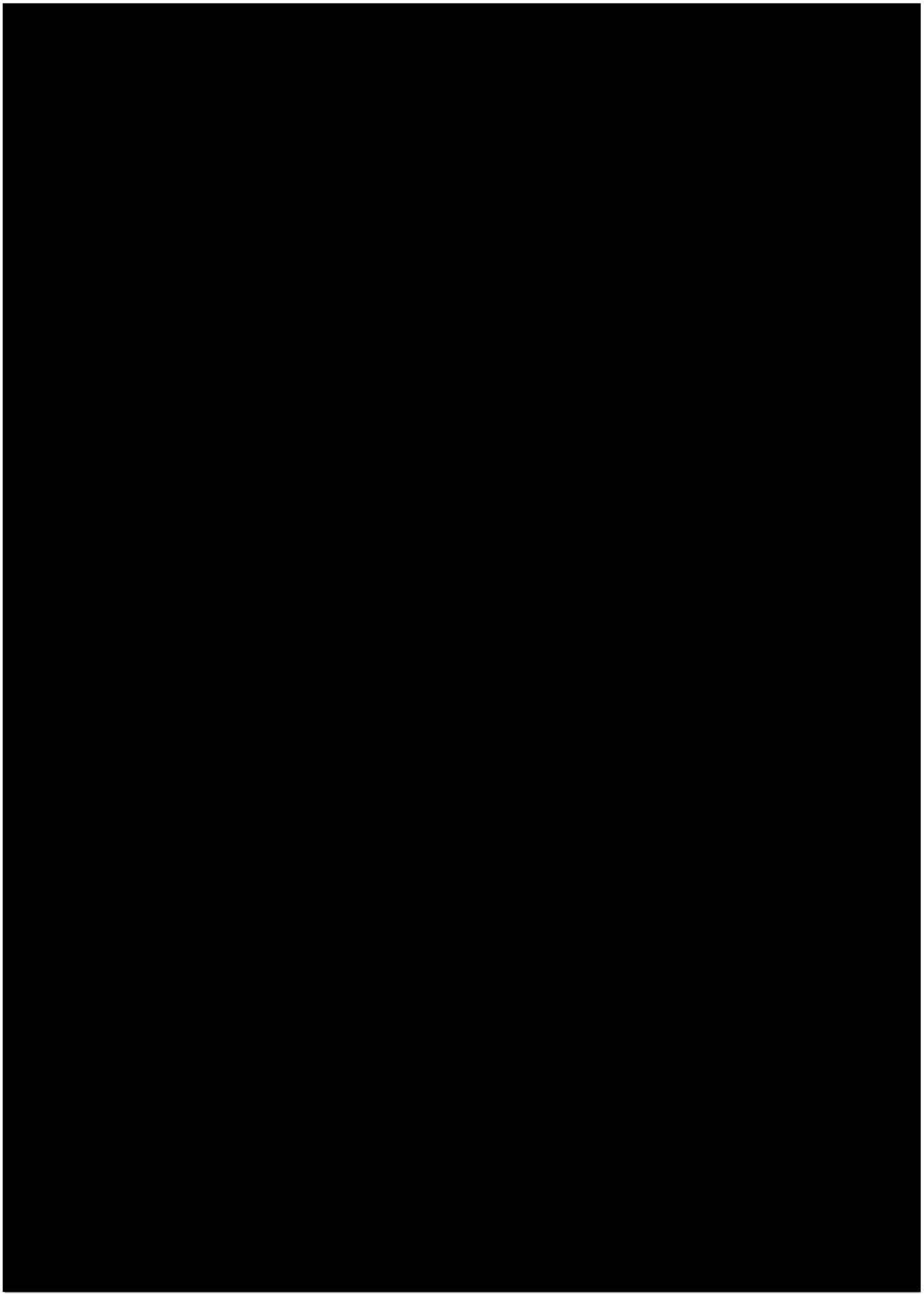
Mika Frances Fryling	Mika	Sept 12, 2014
Program/Department Manager	Signature	Date
Mika Fryling		
Gary B. Munro	Gary B. Munro	Sept 10, 2014
Contact Responsible for Systems Maintenance and/or Security (Signature not required unless they have been involved in this PIA.)	Signature	Date
Gary Munro		
Peter R. Kingston	→	9/18/2014
Head of Public Body, or designate	Signature	Date
Peter Kingston		

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

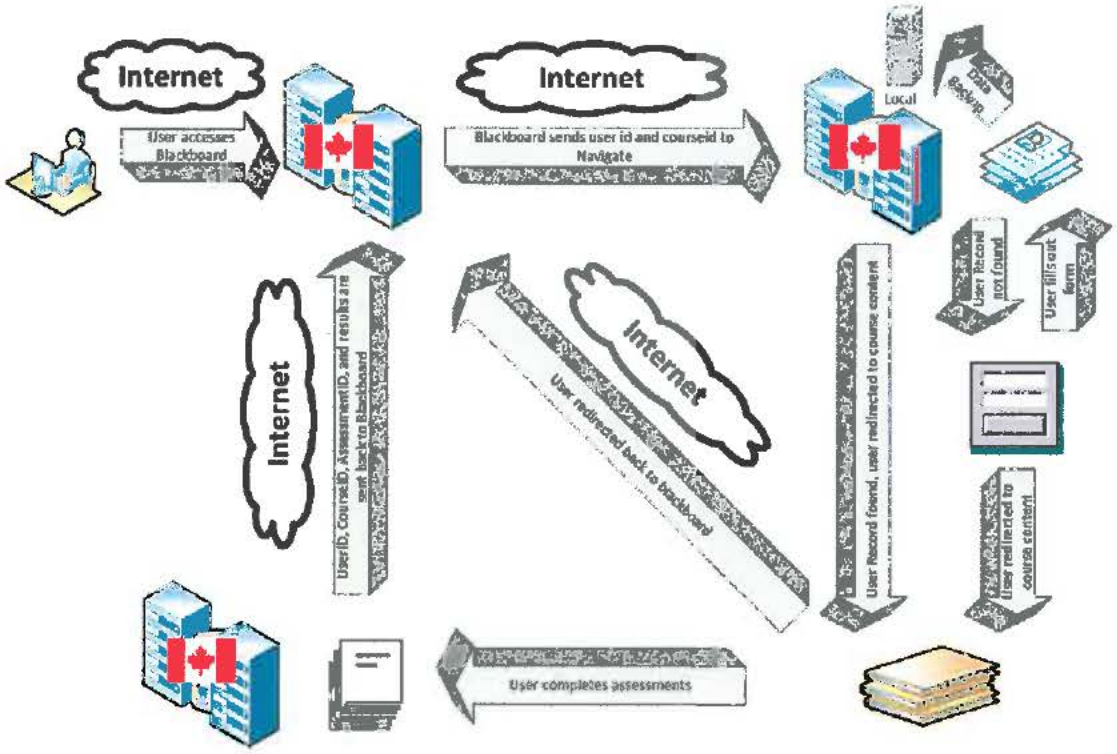
If you have any questions, please contact your public body's privacy office(r) or call the OCIO's Privacy and Access Helpline at 250 356-1851.

S.15(1)(l)





All data centers are located in Canada, and information never travels to any other country.



PRIVACY PROTECTION SCHEDULE

This Schedule forms part of the agreement between The Justice Institute of British Columbia (the "Public Body") and Jones and Bartlett Learning (J&B) (the "Contractor") respecting Navigate materials for Instruction by the Fire and Safety Division of the JIBC (the "Agreement").

Definitions

1. In this Schedule,
   (a) "access" means disclosure by the provision of access;
   (b) "Act" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
   (c) "contact information" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
   (d) "personal information" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Public Body and the Contractor dealing with the same subject matter as the Agreement but excluding any such information that, if this Schedule did not apply to it, would not be under the "control of a public body" within the meaning of the Act.

Purpose

2. The purpose of this Schedule is to:
   (a) enable the Public Body to comply with its statutory obligations under the Act with respect to personal information; and
   (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Public Body otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

4. Unless the Agreement otherwise specifies or the Public Body otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.

5. Unless the Agreement otherwise specifies or the Public Body otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
   (a) the purpose for collecting it;
   (b) the legal authority for collecting it; and
   (c) the title, business address and business telephone number of the person designated by the Public Body to answer questions about the Contractor's collection of personal information.

Accuracy of personal information

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Public Body to make a decision that directly affects the individual the information is about.

Requests for access to personal information

7. If the Contractor receives a request for access to personal information from a person other than the Public Body, the Contractor must promptly advise the person to make the request to the Public Body unless the Agreement expressly requires the Contractor to provide such access and, if the Public Body has advised the Contractor of the name or title and contact information of an official of the Public Body to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

8. Within 5 business days of receiving a written direction from the Public Body to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.

9. When issuing a written direction under section 8, the Public Body must advise the Contractor of the date the correction request to which the direction relates was received by the Public Body in order that the Contractor may comply with section 10.

10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Public Body, the Contractor disclosed the information being corrected or annotated.

11. If the Contractor receives a request for correction of personal information from a person other than the Public Body, the Contractor must promptly advise the person to make the request to the Public Body and, if the Public Body has advised the Contractor of the name or title and contact information of an official of the Public Body to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Storage and access to personal information

13. Unless the Public Body otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Retention of personal information

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Public Body in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

15. Unless the Public Body otherwise directs in writing, the Contractor may only use personal information if that use is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

Disclosure of personal information

16. Unless the Public Body otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Public Body if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

17. Unless the Agreement otherwise specifies or the Public Body otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

Notice of foreign demands for disclosure

18. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.2 of the Act, if in relation to personal information in its custody or under its control the Contractor:
   (a) receives a foreign demand for disclosure;
   (b) receives a request to disclose, produce or provide access that the Contractor knows or has reason to suspect is for the purpose of responding to a foreign demand for disclosure; or
   (c) has reason to suspect that an unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure

   the Contractor must immediately notify the Public Body and, in so doing, provide the information described in section 30.2(3) of the Act. In this section, the phrases "foreign demand for disclosure" and "unauthorized disclosure of personal information" will bear the same meanings as in section 30.2 of the Act.

Notice of unauthorized disclosure

19. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.5 of the Act, if the Contractor knows that there has been an unauthorized disclosure of personal information in its custody or under its control, the Contractor must immediately notify the Public Body. In this section, the phrase "unauthorized disclosure of personal information" will bear the same meaning as in section 30.5 of the Act.

Inspection of personal information

20. In addition to any other rights of inspection the Public Body may have under the Agreement or under statute, the Public Body may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

21. The Contractor must in relation to personal information comply with:
   (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and
   (b) any direction given by the Public Body under this Schedule.

22. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

23. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Public Body of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

24. In addition to any other rights of termination which the Public Body may have under the Agreement or otherwise at law, the Public Body may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

25. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

26. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.

27. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

28. If a provision of the Agreement (including any direction given by the Public Body under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.

29. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or, subject to section 30, the law of any jurisdiction outside Canada.

30. Nothing in this Schedule requires the Contractor to contravene the law of any jurisdiction outside Canada unless such contravention is required to comply with the Act.

JIBC Privacy Notice found at www.jibc.ca/privacy

As at 2014.08.18

Privacy

Freedom of Information and Protection of Privacy Act

The Justice Institute of BC (JIBC) complies with BC's Freedom of Information and Protection of Privacy Act (FIPPA), which allows access to information held by public bodies and determines how public bodies may collect, use and disclose personal information.

The JIBC collects personal information for purposes associated with its operating programs and activities. The Act applies to all records in the custody or under the control of the JIBC, with some exceptions. Requests may be made for access to records containing an individual's own personal information or to records containing general information.

The Act does not apply to some categories of records including:

- A record containing information about a question that is to be used on a JIBC examination or test
- A record containing teaching materials or research information of employees at JIBC

In responding to access requests, JIBC may redact certain information based on the exceptions from disclosure in the Act. See JIBC's Freedom of Information and Protection of Privacy Policy.

For more information about JIBC's privacy procedures, contact:

Vice President, Finance & Administration
Justice Institute of BC
715 McBride Boulevard
New Westminster, BC
V3L 5T4

For more information about FIPPA, which is enforced by the Office of the Information & Privacy Commission (OIPC) for British Columbia, see the OIPC website.

Notice of Disclosure of Personal Information to Statistics Canada

Statistics Canada is the national statistical agency. As such, Statistics Canada carries out hundreds of surveys each year on a wide range of matters, including education. Statistics Canada asks all colleges and universities to provide data on students and graduate. Institutions collect and provide to Statistics Canada, student identification information (student's name, student ID number, Social Insurance Number), student contact information (address and telephone number),

student demographic characteristics, enrolment information, previous education, and labour force activity.

The federal Statistics Act provides the legal authority for Statistics Canada to obtain access to personal information held by educational institutions. The information may be used for statistical purposes only, and the confidentiality provisions of the Statistics Act prevent the information from being released in any way that would identify a student.

Students who do not wish to have their information used can ask Statistics Canada to remove their identifying information from the national database. On request by a student, Statistics Canada will delete an individual's contact information (name, address, or other personal identifies) from the ESIS database. To make such a request, please contact them:

- Email: Esis-siae_contact@statcan.ca
- Phone: 1.613.951.1666 1.613.951.1666 (Monday-Friday, 8am-5pm EST/EDST)
- Mail:
  Post-secondary Education and Adult Learning Section
  Centre for Education Statistics
  Statistics Canada
  Jean Talon Building
  1-B-9 Tunney's Pasture
  Ottawa, ON K1S 0T6

Further details on the use of this information can be obtained from the Statistics Canada website.

JIBC Website and Personal Information

JIBC's web servers, and web analytics services used by JIBC, automatically collect information that is essential to the security, technical maintenance and usability of the JIBC website, hereinafter referred to as the "Site". The information collected includes data such as:

- Browser and operating system type and version used to access the Site
- Internet service provider (ISP) name and Internet Protocol (IP) address of visitors
- Pages visited, including duration, date and time
- Addresses of external websites linked to the Site and used by visitors to enter the Site

JIBC uses the information to maintain security, diagnose technical issues and conduct statistical analysis to assist in making the site more useful to visitors.

The extent of personal information collected by JIBC's servers depends on the standards followed by your ISP. You may wish to contact your ISP to determine the policies and practices in this regard.

Access to information collected is restricted to authorized individuals. JIBC makes no attempt to link the information collected to the identity of individuals.

While viewing portions of the Site, small data files called "cookies" may be stored on your browser to assist you when returning to a specific page or area on the Site. If you have concerns about cookies, you can configure your web browser settings to not accept cookies or to display warning messages.

- All Access

Last updated March 7, 2013

JIBC

Policy No:

Responsibility: **VP Finance & Administration**

Policy - Information Security

Approved by: **Board of Governors**

Effective: **November 22, 2012**

Revisions:

Context

Information and the associated processes, systems and networks are valuable assets of the JIBC and the management of personal data has important implications for individuals. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and/or contractual obligations. The JIBC is committed to the security of information, both within the college and in communications with third parties.

Policy

This policy is intended to protect the security of the JIBC's information assets and is applicable to all JIBC staff, faculty and students.

Definitions

For the purposes of this Policy, "information security" means the preservation of:

a) **Confidentiality** – i.e. protecting information from unauthorized access and disclosure;
b) **Integrity** – i.e. safeguarding the accuracy and completeness of information and processing methods; and
c) **Availability** – i.e. ensuring that information and associated services are available to authorized users when required.

For the purposes of this policy "information" includes all data and information that is printed or written on paper, stored electronically, transmitted by post or using electronic means including cloud based services or social media sites, shown on visual media, or spoken in conversation.

Scope

Compliance with Law or Legislation
The JIBC holds and processes information about employees, students, and other data subjects for academic, administrative and commercial purposes. When handling such information, the JIBC, and those to whom this Policy applies, must be in compliance with the current *BC Freedom of Information and Protection of Privacy Act (FOIPOP) [RSBC 1996]*. Responsibilities under the FOIPOP Act are set out in the JIBC's Freedom of Information and Protection of Privacy Policy.

Responsibilities

1. Information security is the responsibility of all members of the JIBC community. Every person handling JIBC related information or using JIBC information systems is required to observe this Policy and these Regulations.

2. The JIBC's Technology Steering Committee which includes JIBC Executives may establish specific procedures to ensure information security with regard to the JIBC-related information is protected. These procedures may include a matrix that defines who is responsible for the security of certain types of information and the measures required to protect that information.

3. Security Controls – The JIBC will maintain reasonable detection and prevention controls to protect against, and detect instances of, malicious software and unauthorized access to networks and systems. All users of JIBC's computers, including laptops and mobile devices; on which JIBC-related information is kept shall comply with procedures established by the JIBC in order to ensure compliance with legislation and to ensure that up-to-date security controls are maintained on those systems.

4. All members of the JIBC community must report immediately to the Director of Technology Services or their delegate any observed or suspected security incidents where a breach of this policy has occurred.

Procedures

Policy Review
The JIBC's Technology Steering Committee will review and make any recommendations for update of this policy to the JIBC Management Committee before it is submitted to the Board of Governors.

Related Documents

Student Records Policy and Procedures
Student Code of Conduct Policy
Harassment Policy for Employees and Students
Intellectual Property Rights Policy
Records and Information Management Policy
Freedom of Information and Protection of Privacy Policy
Conflict of Interest and Standards of Ethical Conduct

JIBC

Policy No:

Responsibility: VP Finance & Administration

Policy - Information & Educational Technology Acceptable Use

Approved by: Board of Governors

Effective: November 22, 2012

Revisions:

Context

The JIBC provides Information and Educational Technology (IET) resources to JIBC staff, faculty and students to support the teaching, learning, research and administrative goals and functions of the JIBC. These IET resources are valuable community assets which are expected to be used and managed responsibly to ensure their integrity, security and availability for the educational and administrative activities of the JIBC.

Policy

This policy establishes guidelines for both acceptable and unacceptable uses of JIBC owned or leased IET resources, thereby ensuring a stable, effective and efficient operation while minimizing potential disruption and risk.

Breaches of this Policy may be subject to the full range of disciplinary and other formal actions up to and including dismissal. In addition to any other sanctions that JIBC may levy in the event of a violation, JIBC may withdraw computing privileges and network access.

JIBC reserves the right to limit, restrict or extend computing privileges and access to its computing and communications resources, including all information stored therein.

NOTE
This Policy is not intended to set forth an exhaustive list relating to the use of JIBC computing resources. All users continue to be subject to all applicable laws and JIBC policies.

Definitions

INTELLECTUAL PROPERTY

1. Users must respect the legal protection provided by copyright laws for computer programs and data compilations and for all other works (literary, dramatic, artistic or musical). Also, users must respect the legal protection provided by trademark law and the common law for names, marks, logos, and other representations that serve to distinguish the goods or services of one person from another.

2. Users must respect the rights of others by complying with all JIBC policies regarding intellectual property regardless of medium (i.e. paper or digital).

FREEDOM OF EXPRESSION

Users should be aware that, while the JIBC has programs to screen emails for viruses, worms etc., its practice is not to control the information available on our campus network.

HARASSMENT

All users must comply with the JIBC Harassment Policies

EXAMPLES OF ILLEGAL USES

The following are representative examples only and do not comprise a comprehensive list of illegal uses:

- Uttering threats (by computer or telephone);
- Accessing, storing or distributing child pornography; and
- Copyright infringement.

EXAMPLES OF UNACCEPTABLE USES

The following are representative examples only and do not comprise a comprehensive list of unacceptable uses:

- Use of the JIBC's IET resources for outside business, commercial or non-incidental personal use is prohibited unless such use is sponsored and approved by the JIBC.
- Seeking information on passwords or data belonging to another user;
- Making unauthorized copies of proprietary software, or offering unauthorized copies of proprietary software to others;
- Distribution of pornographic materials (exception: those with a legitimate academic purpose for doing so may distribute such material for a stated legitimate academic purpose);
- Copying someone else's files, or programs, or examining such information unless authorized;
- Attempting to circumvent computer security methods or operating systems (e.g. subverting or obstructing a computer or network by introducing a worm or virus);
- Using JIBC-provided computer accounts for commercial purposes such as promoting by broadcast non-educational profit-driven products or services;
- Intercepting or examining the content of messages, files, or communications in transit on a voice or data network;
- Adding unauthorized servers, network devices, or any unauthorized electronic devices that could compromise the security of JIBC electronic information

- Interfering with the work of other users of a network or with their host systems, seriously disrupting the network (e.g. chain letters or spamming), or engaging in any uses that result in the loss of another user's files or system; and
- Gambling, betting, or pyramid schemes;
- Harassing, discriminatory messages including cyber-bullying.

SYSTEM ADMINISTRATORS

Subject to 'Privacy and Security Section 2' above, this policy shall not be construed as preventing or restricting duly authorized system administrators or other technical personnel from carrying out their duties. Complaints regarding this section of the policy may be directed to the Director of Technology Services.

Scope

This Policy and related Procedures apply to:

- All JIBC owned or leased IET resources including networks, information systems, applications, computers, Smartphones, tablets and other communication devices and information assets.
- Any member of the JIBC community including students, employees and other individuals or organizations that uses JIBC IET resources on or off Campus.
- The use of personal equipment (e.g. laptop, smartphones, tablets, etc.) connected to the JIBC's data & voice networks.
- User-created content through online publishing and discussion including blogs, wikis, file-sharing, user-generated video, audio, virtual worlds and social networks sites.
- Portable storage devices such as external hard drives, USB flash drives, CD-ROM, DVD-ROM

Procedures

RESPONSIBLE USE

1. Computer IDs, accounts, and other communications facilities or equipment are to be used for authorized purposes. Subject to any JIBC Conflict of Interest policies, limited personal use is acceptable if it does not interfere with use of the facility for its intended purpose and, in the case of employees, if does not interfere with job performance.

2. Users are responsible for the use to which their computing accounts are put. Users must not share their login credentials (username and password) for any accounts to which they have access.

3. Users are prohibited from accessing other users' computer IDs or accounts and communications, without specific prior authorization of the user and from the appropriate Director, Dean or Vice - President.

4. Users must not misrepresent their identity as senders of messages or alter the content of such messages with intent to deceive.

5. All users must adhere to JIBC policies and all legislation that govern the use of JIBC's computing and communication facilities. Applicable legislation includes, but is not limited to, the Criminal

Code of Canada, the B.C. Civil Rights Protection Act, the Canadian Copyright Act, the B.C. Freedom of Information and Protection of Privacy Act, and the B.C. Human Rights Code.

6. Users must not use JIBC's information technology facilities and assets for activities like gambling, betting, pyramid schemes, personal gain or illegal activities.

PRIVACY AND SECURITY

1. Users must:
   a. Preserve the privacy of data to which they have access in accordance with applicable laws and the JIBC's policies including our Freedom of Information and Protection of Privacy Policy;

   b. Respect the privacy of others by not tampering with email, files, or accounts they use; and

   c. Respect the integrity of computing systems and data.

   d. For example, users must not: intentionally develop programs or make use of already existing programs to harass or bully other users, infiltrate a computer or computing system, damage or alter the components of a computer or computing system, gain unauthorized access to other facilities accessible via the network, or inappropriately use the telephone system.

   e. JIBC confidential or private information classified under the BC Privacy Act must not be downloaded to insecure or unencrypted media such as laptops, storage devices (USB's, external hard drives, etc.). smartphones, tablets or other types of electronic devices

   f. Although electronic records on JIBC equipment are the property of JIBC and JIBC is entitled to review those records, the user community can be assured that system administrators will not examine electronic files without the individual's prior knowledge, except in emergencies or under extenuating circumstances. In no event will JIBC personnel examine other users' electronic files without authorization in writing from a member of the JIBC executive.

Related Documents

Student Records Policy and Procedures
Student Code of Conduct Policy
Harassment Policy for Employees and Students
Intellectual Property Rights Policy
Records and Information Management Policy
Freedom of Information and Protection of Privacy Policy
Conflict of Interest and Standards of Ethical Conduct

JIBC

Related Policy: Student Records Policy
Policy No.
Procedure No.
Responsibility: Registrar

Procedure – Creation, Maintenance and Retention of Student Records

Approved by: Management Committee
Effective: 12/5/2007 (replaces Student Record Guidelines & Procedures 7/11/00)
Revisions:

An Official Student Record is generated for each student. In some cases, such as very short courses, conferences or examinations without coursework, creation of a record for each student may be impractical and may be waived by the Division Director or the Registrar. Documentation of student course attendance and achievement is usually in the interest of both the student and the Institute. The required information should be recorded and maintained whenever possible.

1 Creation and Retention of Applicant Records

1.1 An applicant record is created as an active record when an applicant requests orally, in writing or electronically to be enrolled in a program, course or other student service. An applicant record is a temporary record and is retained as an active record until superseded or obsolete. It may be stored as an electronic file, paper file or both.

1.2 An applicant record may include but is not limited to such items as completed application forms, transcripts from other educational institutions, applicant exam results, criminal record investigation results, reference letters, telephone reference notes, medical records and releases, assessment centre notes, psychological assessments and interview notes.

1.3 An applicant record must contain:

- documentation regarding the final determination of the application, such as a copy of a letter sent to the student confirming whether admission was granted or denied; or
- a notation on the file indicating what, how, when and by whom the student was advised.

1.4 Where an applicant is admitted as a student, the applicant record is purged of obsolete information such as interview notes and reference letters at the time of admission. The remaining information forms part of the Official Student Record

1.5 Where an applicant is not admitted as a student, the applicant record is retained as a record until the end of the established appeal period, or, where no appeal period is specified, for a period of two years. An applicant record may be retained past the end of the established appeal period or for more than two years, if this is determined to be appropriate by the responsible Division Director.

2 Creation, Maintenance and Retention of Student Records

2.1 Creation and maintenance of student records is a distributed function based on the use of a shared electronic student database. This means that different elements of a student record may be created or modified by designated staff from a variety of Divisions. In most cases this will include staff from relevant program areas, Financial Services, and the Registrar's Office.

2.2 It is the responsibility of the Division to ensure that any staff member designated to create and maintain student records is qualified, properly trained and aware of the importance of maintaining the integrity of student records and protecting the privacy of the information contained in the record.

2.3 A student record is initiated as an active record when a student is accepted for enrollment into a program or course. The student record includes information held by the Institute regarding any student who has enrolled in a course, program, examination or other student service. A complete student record includes both the Official Student Record and temporary records. Student records may be stored as electronic files, paper files, or both.

2.4 An active record normally becomes inactive on the date that a student completes or withdraws from a program or course. At the end of the established appeal period, or, where no appeal period is specified, a period of two years, the inactive record is purged of temporary records and only information that is to be part of the Official Student Record is retained.

2.5 A temporary student record may include but is not limited to such items as: application records, correspondence, interview notes, reference letters, telephone reference notes, psychological assessments, student exam papers, student assignments, lists of student assignment grades, exam schedules, class lists, class transfer documents, counseling records and financial assistance records

2.6 The Official Student Record consists of the information required to produce an Official Student Transcript. It may contain additional information such as telephone numbers, e-mail addresses, gender, date of birth, aboriginal status, disability, citizenship, entrance test scores, prior learning assessment results, entrance requirements data, narrative evaluations, and records of academic misconduct and academic distinction and other information that a Division Director explicitly identifies as appropriate for that Division.

2.7 The Official Student Record is retained as an active record while the student is registered in a course or program, plus one year. At the end of one year, the Official Student Record becomes semi-active and is retained for a period of sixty (60) years. A log indicating the location of the records is maintained as an active administrative record.

2.8 The Institute may develop systems that enable students to enter and modify some personal information on their own student record. For example, students may be granted permission to amend address information electronically through the Internet

3 Special Notations

3.1 Academic Distinction

3.1.1 Academic Distinction is a level of excellence in student achievement recognized by the Institute as worthy of special notation on the Official Student Record. Program Council approves all academic distinctions that are to be recorded on the student transcript.

3.1.2 An Academic Director advises the Registrar's Office of recipients of Academic Distinctions. In consultation with the Division and the approval of Program Council, the Registrar's Office creates the appropriate Academic Distinction notation and enters it into the student's electronic record. Academic Distinctions are printed on the Official Student Transcript.

3.2 Academic and Non-academic Discipline

3.2.1 An academic or a non-academic discipline notation may be made on a student record for conduct that is deemed by an Academic Director to be in violation of the Institute's Student Code of Conduct or other policy. Discipline may include oral cautions, written letters of warning, written reprimands, suspension or expulsion.

3.2.2 The Academic Director determines the need and duration for a disciplinary notation on a student's record and advises the Registrar's Office. In consultation with the Director, the Registrar's Office creates the appropriate discipline notation and enters it into the student's electronic record. Discipline notations may be permanent or limited to a specified period of time.

3.2.3 In accordance with standards recommended by the BC Public Post-Secondary Institution Senior Educational Services Officers Committee (SESOC) in November 2001 and approved by the BC Registrar's Association (BCRA) in November 2002, the following student transcript notations will be used in cases of disciplinary dismissal:

- Academic Discipline
- Non Academic Discipline

3.2.4 The notation appears on the Official Student Transcript either permanently or for a specified time period.

3.2.5 The Registrar's Office reviews disciplinary entries periodically and deletes those for which the established time period has expired. In such cases, reference to the discipline is removed from both the transcript and the student record.

3.2.6 When issuing an Official Student Transcript, the Registrar's Office reviews the student record to ensure that only discipline notations that have not expired are included.

3.2.7 After a period of seven (7) years, a student may request the removal of a permanent disciplinary notation from his/her record. The decision to approve the request for removal of a permanent disciplinary notation will be made by the Registrar after consultation with senior management of the Institute as appropriate.

4 Retention of Course Outlines

4.1 Course outlines are retained, as semi-active files, by the Division for sixty years after they are superseded because they retain primary (operational) value for describing courses offered by the Institute in the past. A log indicating their location must be maintained as an active administrative record.

Related References

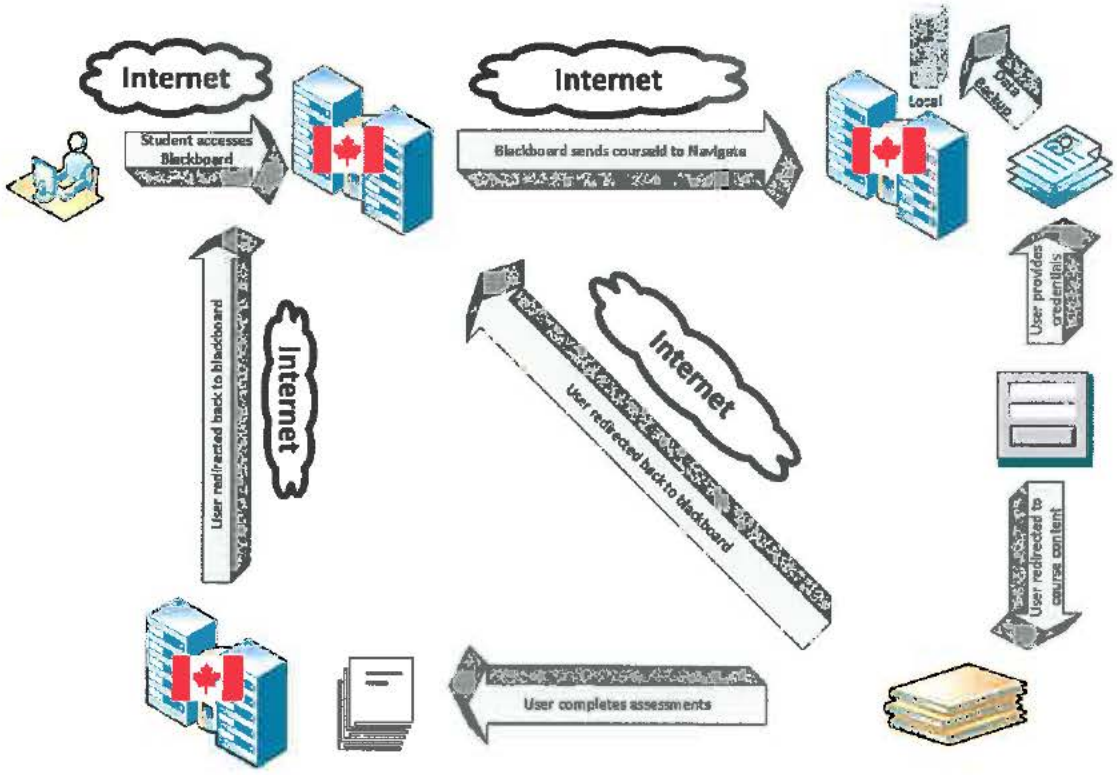
- Freedom of Information and Protection of Privacy Policy
- Protection of Privacy of Student Information
- Student Code of Conduct

A student logs in to Blackboard using his/her login credentials. When a user is presented with a course content that is hosted on Navigate, Blackboard sends a request to Navigate with the course id.

Navigate receives the information and validates the oAuth signature of the request. If the validation fails then an error will be returned.

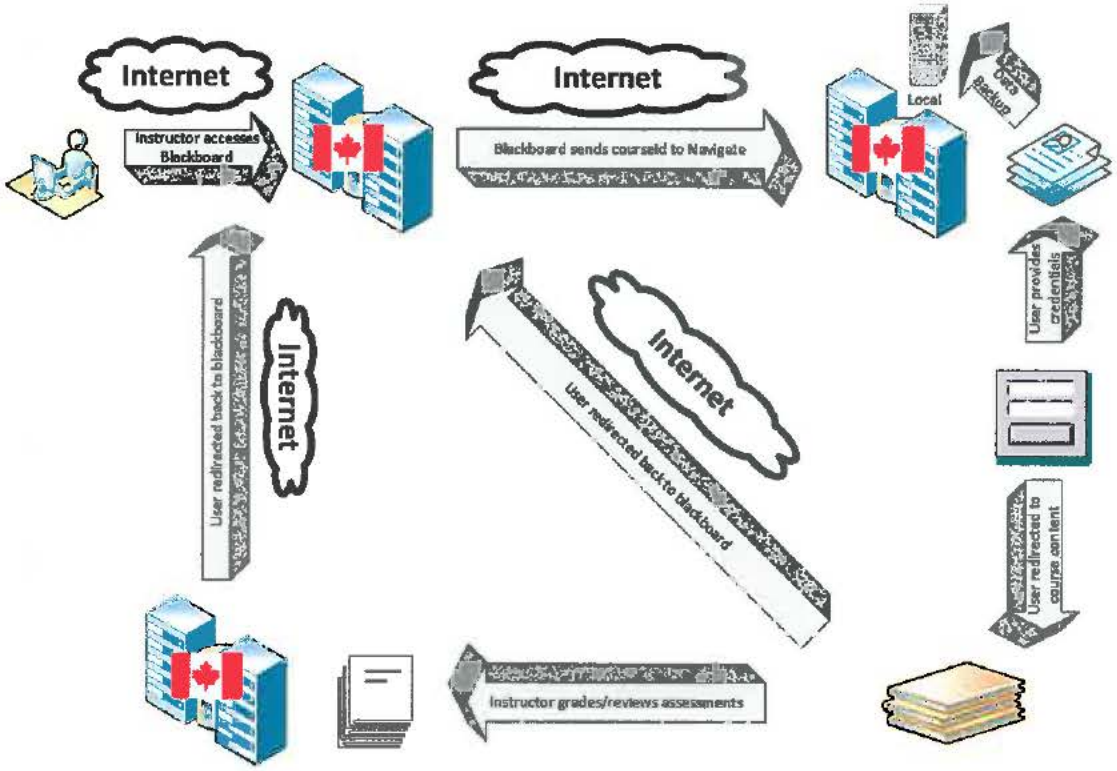
Navigate prompts the user to provide his/her credentials. If this is a new user, the user is prompted to provide more information. This information is defined by the institution/organization to which the user belongs.

After the user is authenticated, he/she is redirected to the course content. If the course requires assessments, the user completes the assessment.



LL Note: – Confirmed on 2014.08.28 that when BlackBoard is mentioned in this document, it refers to JIBC's local installation of BlackBoard and that the Moodle reference on page 2 is to be ignored and/or replaced by the word "BlackBoard" Assessments, quizzes, exams are administered locally.

The instructor logs in to Moodle, and he/she can view the list of courses they currently teach. Instructors can view students' grades and export them to a csv file.



All information that travels over the Internet is secured using oAuth, and no personally identifiable information is ever passed.

Backups for user records are made locally on a daily basis.

All data centers are located in Canada, and information never travels to any other country.