Educational Technology Privacy Compliance

Procedure No:	5900-PR3
Policy Reference:	5900 – Educational Technology Policy
Version:	1
Category:	Education
Approving Body:	Board of Governors on advice of Education Council
Executive Sponsor:	Chair of Education Council
Department Responsible:	Education
Directory of Records Class:	0650-15
Approval Date:	2021 April 21

Objectives

The use of Educational Technologies (ET) may require the sharing, processing, and storage of BCIT Protected Information. Compliance with regulations governing the protection of the personal information of students and other stakeholders is paramount when planning for the use of any ET at BCIT.

To ensure the protection of personal information all uses of ET are required to meet the requirements of the Freedom of Information and Protection of Privacy Act (FIPPA) Part 3 – Protection of Privacy. In addition, all uses of ET are required to be in compliance with Policy 6700 – Freedom of Information and Protection of Privacy.

The purpose of these procedures is to outline the basic steps necessary for users of ET to follow when planning their use of new or updated ET.

The steps outlined in this policy will not ensure the use of an ET is in compliance with associated BCIT policies. Users of ET are required to have their use of an ET approved by the BCIT Information Access and Privacy Office as to matters of Protected Information.

Who This Procedure Applies To

All evaluators, decision makers and users of BCIT's ET.

Scope

Protection of privacy is a requirement for the use of all ET regardless of the model of use or type of user. This procedure applies to:

- All internal or external ET not previously assessed for privacy risk and approved for use.
- All models of use, for both institutional and ad hoc ET.
- Previously approved ET will be re-assessed for privacy risk as a consequence of a change in the model of use. This includes, but is not limited to:
  - Changes to the way existing features are being utilized by BCIT faculty as part of their course delivery (model of use).

  - Additional features being added to the ET by the vendor, which may be adopted for use with students.
- All ET in use at BCIT must be re-assessed for privacy risk as a consequence of vendor upgrades to an ET. This includes, but is not limited to:
  - Changes to functionality resulting in the types of student data being sent to, processed by, or stored by the ET.
  - Changes to models of integration with BCIT systems.
- All ET in use at BCIT must be re-assessed for privacy risk as a consequence of a change in the manner and or location of BCIT data transfer, processing, or storage.
- All ET in use at BCIT must be re-assessed for privacy risk as a consequence of a change to the vendor's Terms of Use (license).
- All ET in use at BCIT must be re-assessed for privacy risk as a consequence of a change to the ownership or control of the ET.

Regulations Governing Privacy Compliance

- BCIT Policy 6700—Freedom of Information and Protection of Privacy
- BCIT Policy 3502 – Information Security
- British Columbia *Freedom of Information and Protection of Privacy Act* (FIPPA)

Procedures

Step 1: Assess the Risk

All ET being considered for use at BCIT will be assessed for privacy risks prior to pilot or institute implementation and operationalization. Because ET can be used in different ways by different faculty (the model of use), the risk assessment will:

- Be conducted by the stakeholder(s) proposing the ET for use.
- Be supported, as appropriate, by other stakeholder groups as identified in policy 5900 – Educational Technology.
- Assess privacy risks associated with access to, and the use of, the ET.
- Assess privacy risks associated with the model of use chosen by the faculty.

Progressive Levels of Risk Assessment

1) **Privacy Compliance Checklist** (PCC) is a simplified form that will be used as a first step in risk assessment. The PCC can, in most cases, be completed by the faculty planning to use the ET from information available through the vendor's web site, and by defining the planned model of use and risk mitigation strategies. The PCC will result in the approval of the ET, with or without conditions of use, or will determine if a more detailed assessment is needed. In most cases, a PCC can be completed within a month.

2) Privacy Impact Assessment or “PIA”: has the same meaning as in the Act, i.e. an assessment that is conducted by BCIT to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3 of the Act.

Step 2: Mitigate the Risk

Where possible, known risks will be mitigated by making adjustments to the ET configuration, integration with other BCIT systems, or the model of use.

One of the risk factors Included in the model of use is the degree to which BCIT requires the use of an ET.

Required for use occurs when an ET is stated as necessary for the successful completion of the course. In such cases, the following steps will be taken:

- The requirement and associated risk will be declared in the information used by students when making a decision prior to registering for the course, or applying to the program, in which the ET is used.
- The details of the risk will be communicated to the students on the first day of the course.
- Students will be provided with an opt-out alternative that doesn’t compromise their learning.
- Students will be given the choice to accept the risk and use the ET, or use the opt-out option without any penalty.

Recommended for use occurs when the use of an ET is recommended for successful completion of the course. In such cases BCIT carries the same obligations as if the ET were Required for use.

Optional use occurs when students have complete discretion to use, or not use, an ET.

Optional use carries no BCIT burden of privacy protection beyond the communication of privacy and cyber security awareness. Faculty providing optional ET resources to their students will include:

- A general statement advising students of general privacy considerations when using any cloud based application.
- A notification that the use of any of the listed resources is at the students own risk.

Step 3: Declare the Risk

In cases of required or recommended use, after the known risks have been mitigated the remaining risks will be explained to students in a manner that they can understand with an opportunity to ask questions.

Students will then be allowed to choose to accept the risk by providing their informed consent for use, or to refuse to accept the risk and select and opt-out option. The Risk declaration will be provided by one of the following:

- **Mini-lesson** delivered in a face-to-face or real-time virtual lesson.
- **Self-paced reading** in an online course.

Step 4: Provide an Opt-out Option

Students choosing not to accept the declared risk will be provided with an alternative way of achieving the same learning outcomes as those facilitated by the ET. This may include, but is not limited to:

- Alternative and more privacy compliant ET.
- Alternative access to the same information.
- Alternative means of completing the learning activity facilitated by the ET.

Where no reasonable opt-out option exists where use of the ET is required as part of a program of studies, students will be informed of the requirement to use the ET and the associated risk to personal information prior to making the registration decision. This enables the prospective student to make an informed decision as to how to balance the risk to their privacy against their desire to enroll in the course or program before making the commitment and starting the learning. In such cases, instructors are still required to follow steps 3 and 5 at the start of the course(s) using the ET.

Step 5: Secure Informed Consent

Informed student acceptance, of any privacy risk arising from the use of a recommended or required ET, be documented and archived.

Students will be informed of any risk to their privacy through a short lesson or online reading that explains the ET and how it will be used in the course, the nature of the risk, and any risk mitigation strategies in use.

Acceptance must occur through one of the following:

- **Physical**: A printed consent form will be signed by the student.
- **Digital**: A single question quiz, in the online course, that requires the students to read the risk declaration and answer Yes or No to the following:

  I have read, understand, and accept the risks associated with my use of <name of ET>, in use in my BCIT course <course number and name>.

Archival of the consent will occur through one of the following means:

- **Physical** acceptance forms will be retained by the program for 4 terms after the student completes the course or program in which the accepted ET was included.
- **Digital** acceptance requires no action. The student response to the quiz question will be automatically retained by the Learning Hub course archive.

Amendment History

			Approval Date	Status
1.	Created:	Procedure 5900-PR3 version 1	2021 APR 21	Active

Scheduled Review Date

2021 APR 21