Privacy Impact Assessment (PIA) for PebblePad

Before you start

- This Privacy Impact Assessment (PIA) form is used by VCC to assess whether a new initiative, or proposed significant change to an existing initiative, meets the privacy protection requirements of the B.C. *Freedom of Information and Protection of Privacy Act.* FIPPA's protection of privacy requirements. A PIA is a legislative requirement (FIPPA s. 69(5.3)) and mandatory before implementing an initiative.
- You/Your refers to the individual responsible for drafting this PIA, who should be an individual from the relevant department or program area with sufficient knowledge to do so. The PIA must be signed by the role within the program area with the appropriate position to hold accountability for this initiative.
- Please include references to other documents when applicable, but do not insert or embed any documents to/in this assessment form.
- Please review the initial assessment questions and contact the Privacy Office at privacyandfoi@vcc.ca before you begin the form, if you have not already. See more guidance about the PIA process, including the supplementary Guidance Document, on the myVCC Privacy website.

PART 1: GENERAL INFORMATION

PIA file number: 2025-009

Initiative title:	PebblePad (ePortfolio system)
VCC Department / Program Area:	Centre for Teaching, Learning, and Research
Link to VCC initiative website:	n/a
Link to vendor website:	https://pebblepad.com/
Link to vendor privacy policy:	https://pebblepad.com/en-gb/privacy-policy-product/
Your name and title:	Andrew Dunn, Manager, Online Learning Strategy and Design
Your work phone and email:	adunn@vcc.ca
Initiative Lead name and title:	Andrew Dunn, Manager, Online Learning Strategy and Design
Initiative Lead phone and email:	adunn@vcc.ca

General information about the PIA:

Is this initiative a data-linking program under FIPPA? See the definition in Schedule 1 of FIPPA. If this PIA addresses a data-linking program, the Privacy Officer must submit this PIA to the Office of the Information and Privacy Commissioner.	No
Is this initiative a common or integrated program or activity? See the definition of Schedule 1 of FIPPA. Under section FIPPA 69 (5.4), the Privacy Officer must submit this PIA to the Office of the Information and Privacy Commissioner.	No
Does this initiative involve a regular or systematic exchange of personal information between organizations? If yes, this initiative may require an Information Sharing Agreement.	No
Related PIAs, if any: BCNET PebblePad PIA (2021)	

1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved, and when or how long your initiative runs. If this is a change to an existing initiative, please also explain the change and the benefits of the change.

VCC is adopting PebblePad, an online portfolio and personal learning platform, for use by students and instructors in specific courses at VCC. VCC licences PebblePad through its membership with BCNET, under the BCNET-PebblePad Licence Agreement (2021). VCC's Centre for Teaching, Learning, and Research is responsible for administering PebblePad at VCC.

VCC's instance of PebblePad will integrate with Moodle as determined by PebblePad administrators (CTLR). Although it is possible for any VCC Moodle course to be linked to a PebblePad workspace, only some selected VCC courses will integrate with PebblePad s. 13(1) , where it has been determined there is a pedagogical need to use the platform. VCC has s. 21(1) licences for both students and employees that will be used only with the VCC courses where PebblePad has been selectively enabled. PebblePad will not be available to students or instructors unless they are participating or instructing one of the selected courses/programs.

PebblePad "can be used by an individual to support their own learning or professional development, or by an organisation to facilitate the learning of their members." PebblePad consists of three components:

- Pebble+: The Personal Learning Space; each user has a personal, private Pebble+ account where users may create records/assets. Every Pebble+ account is private unless the user chooses to share assets or the account with other individuals, the web, or for assessment.
- ATLAS: The institutional assessment space. When users are asked to create items in Pebble+ specifically for assessment or validation, these assets are normally submitted to "Workspaces" within ATLAS so that instructors or other assessors can view them and add feedback, grades, approvals, etc. A Workspace can also be used to provide access to resources, online discussions, and other information relevant to the learning activities within a program of study. (Pebble+ Help source)
- PebblePocket: The free iOS and Android app that users may voluntarily download and use on any mobile device with an internet connection. PebblePocket enables the user to record and collect evidence of experiences (photos, video, audio, notes, reflections) offline.

PebblePocket is included in the software applications covered by the Licence Agreement. PebblePocket does not have full Pebble+ functionality. It is designed to support the creation of records of experience and photo and video evidence while on the run. Assets can be created offline and stored on the mobile device until the learner has connectivity and can send the assets through to their Pebble+ account. (PebblePocket – Pebble+ Help source)

PebblePad can be used for both academic and professional purposes. Some examples of VCC's intended uses include but are not limited to:

- Supporting work-integrated learning through providing a scaffolded structure that allows for external assessment.
- Supporting competency-based assessment through aligning PebblePad content with competency frameworks.

- Supporting portfolio-based pedagogies through allowing students to create and disseminate portfolios that demonstrate their learning.

This PIA largely relies on BCNET's 2021 PIA and BCNET's Licence Agreement with PebblePad, which includes a Privacy Protection Schedule and a Security Schedule. BCNET's PIA describes PebblePad as the following:

> "Designed by educators, PebblePad is used to support learning and professional development by students, employees and professionals. The system provides portfolio and presentation functionality to showcase experience, skills and capabilities of students, while facilitating the tracking of real learning, with personal and professional development. PebblePad also includes a range of tools, services and supports to assist learners in planning, developing and sharing unique attributes. The system is flexible (self-directed or via structured assignments) and can be seamlessly configured to the requirements of any member organization. Functionality and key features of PebblePad includes:
>
> - Learning e-Portfolios – shareable portfolios to showcase and document evidence-based presentations, experience, skills and capabilities (curricular, co-curricular and in between)
> - Learning Templates – recording, reflection and tracking of learning on any device
> - Learning Workbooks – mapping of detailed, shareable digital learning frameworks with progress monitoring capabilities
> - Learning Resources – real-time, reusable and specialized resources for collaboration and professional development
> - Learning Toolkit – intuitive unique design toolkit with media enabled content for learners and teachers
>
> PebblePad retains and archives every record of learning and experience together in a single, secure collated area (e.g. placement journals, collaborative blogs, activity logs, completed module workbooks, uploaded media, performance reviews, feedback, etc.). All users can transfer their content to a free PebblePad personal account when graduating, encouraging lifelong learning and seamless transition from education to career.
>
> The platform also includes a fully integrated, versatile administration and assessment engine to facilitate:
>
> - Design of competency frameworks
> - Authentic, timely feedback and conversations from peers, professionals and faculty
> - Hosting of tools to support formative and summative assessment (e.g. integrated rubics, scorecards, peer review and multi-level approvals)
> - A full suite of reporting including the functionality to demonstrate graphically the stage where learners are, specifically in relation to clinically accredited courses.
> - Access to external expert engagement to contribute and add value to the entire assessment process.
>
> PebblePad allows post-secondary institutions to create an integrated and inclusive work-based learning solution that supports accreditation, appraisal and employability. It is based on transformative technology, mobile-first design and an intuitive interface that connects users and streamlines processes with complete end-to-end functionality. PebblePad is a unique and collaborative platform that directly informs engagement, performance, retention and productivity of students. The system supports the core mission of higher education, is viewed as a foundational

> service for BCNET members and pivotal to an optimum learning experience. PebblePad provides unparalleled specific functionality in support of the post-secondary sector's vision of providing world-class education and research programming.
>
> PebblePad provides a cost-effective, reliable and controlled platform with straightforward licensing as a cloud-hosted solution. Integration with other systems, badge platforms and VLEs [Virtual Learning Environments, or Learning Management Systems] provides flexibility and increased functionality for post secondary education institutions. PebblePad can be accessed via single sign-on (via Active Directory) and seamlessly integrates with Moodle. […]
>
> Founded in 2003, PebblePad is a UK based e-learning technology firm specializing in e-portfolio, e-assessment and personal tutoring systems. In 2016, a new version was launched with an improved interface, workflows and in an HTML5 format. PebblePad supports a wide range of integrations and was the first certified LTI 2.0 portfolio platform. The system is used by a diverse range of institutions internationally including Duke, Columbia and McMaster Universities. PebblePad has been recognized as a global leader in personalized learning for the higher education sector receiving ALT's Learning Technologist of the Year 2007, the 2010 IMS Global Impact Award and the Shropshire Business of the Year for 2011." (BCNET PIA)

2. What is the scope of the PIA?

Your initiative might be part of a larger initiative or might be rolled out in phases. What part of the initiative is covered by this PIA? (An initiative may require multiple PIAs.) What is out of scope of this PIA?

This PIA covers the use of PebblePad as an ePortfolio platform available at VCC and the collection, use, and disclosure of personal information within this platform and its components (Pebble+, ATLAS, and PebblePocket). VCC is a member of BCNET but responsible for its own privacy and security measures. The PIA also considers how VCC's instance of PebblePad integrate with Moodle to share information related to users' account creation and grades, by linking a PebblePad workspace with a course in Moodle.

Beyond the basic amount needed for the creation of user accounts, the amount of personal information collected and used by PebblePad depends on each user's use of PebblePad and the type of content/assets they provide to the system, and whether users use PebblePad for personal use or also for learning/assessment/professional development, which may involve feedback, assessment, and grades from faculty and students.

3. What are the data or information elements involved in your initiative?

*Please list **<u>all</u>** the elements of information or data that you might **<u>collect, use, disclose, store, or access</u>** as part of your initiative (**<u>including but not limited to personal information</u>**). Please:*

- *include where the information is coming from (e.g. collected directly from users, pulled from existing databases, etc.);*
- *group different categories of people together (e.g. students, employees, alumni, etc.) if your initiative involves large quantities of information or datasets.*

In this context, the personal information is that which is required and provided directly from individuals to participate in any VCC activity or program and then utilized in PebblePad.

Collection of personal information from the individual is administered by VCC during the onboarding and registration process. VCC is responsible for the secure transmission of the data between Banner (student and employee information system), Moodle, and PebblePad.

Category	Data or information elements	Source
Student information	**Account information:** Full Name Email address (VCC; personal email if creating an alumni account) Role in Moodle (Student) Course/Module Context (used by PebblePad to register student in appropriate ATLAS workspace) User ID (unique identifier from Moodle, pseudonymized but consistent for grade sync) **Additional information:** Password Username (student ID or alumni account) Reflections, opinions, thoughts on PebblePad material Student work product (which may contain personal information, including audio and video recordings, opinions/reflections, or other PI or third-party PI depending on product) Student grades/feedback/assessment (via faculty/instructor, students or an external professional) Activity timeline and history Area of Study; Course history and details Optional link to personal OneDrive or other third-party drive Profile photo (optional)	PebblePad receives account information via integration with Moodle and Banner upon account creation. Additional information/content in PebblePad is collected directly from student.
Employee information	**Account information:** Full name, email Role in Moodle (Instructor) Course/Module Context (used by PebblePad to register instructor in appropriate ATLAS workspace) User ID (unique identifier from Moodle, pseudonymized but consistent for grade sync) **Additional information:** Feedback and instructor assessments Unique identifiers (e.g. employee ID) Photos, audio and video recordings, opinions/reflections, and any other potential personal information contained in user content (profile/portfolio, assets, etc.) Profile photo (optional)	PebblePad receives account information via integration with Moodle and Banner upon account creation, when an employee follows a link from their Moodle course to PebblePad (when enabled). Additional information/content in PebblePad is collected directly from the employee.
External user information	Name, email address Feedback/comments on shared assets (if permitted)	Collected from external user and submitted by PebblePad user or ATLAS Workspace manager
User/device information	IP address; login information; browser type and version; time zone setting; browser plug-in types and versions; operating system and platform; information about visits, including pages viewed or searched for; page response times; download errors; length of visits to certain pages; page interaction; methods used to browse away; URLs/ clickstreams; crash logs (PebblePocket)	Collected directly from user/user's device

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference. This includes, but is not limited to:

- *Names, home addresses, emails, and telephone numbers of the individual or their guardians and family members (this includes student names and emails!);*
- *Images of an individual;*
- *Identifying number (e.g. student number, employee number, health care number);*
- *An individual's personal views or opinions, or anyone else's opinions about an individual;*
- *Educational, medical, medical, criminal, financial, or employment history.*

Yes.

- If yes, are all of the personal information elements **necessary** for your initiative?
    - **Yes**, then skip question 4 and continue to Part 2

4. If you answered "no" to question 3.1: How will VCC reduce the risk of unintentionally collecting personal information?

Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in a privacy breach or other privacy incident. After you answer this question, submit this PIA to the Privacy Office. You do not need to complete the rest of the PIA template.

N/A

PART 2: COLLECTION, USE, AND DISCLOSURE

This section will help you identify the legal authority for collecting, using, and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use, and disclosure flow

Describe the information flow of your initiative in the chart below. The table explains the movement of personal information throughout your initiative (column 1) and identifies each time personal information is collected, used, or disclosed (column 2) and under which corresponding FIPPA authority (column 3).

Use column 4 if there are any specific potential risks related to each step. Change the information flow and add more rows as necessary. The red text below is an example – input the steps and relevant authorities to reflect your initiative's flow.

For the most common FIPPA authority references to assist with completing this chart, please see Section 1 of the Guidance Document, or consult the full text of Part 3 of FIPPA.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FIPPA authority or other legal authority**	**Specify any potential risks**
Users (students and instructors) follow a link to access PebblePad via their Moodle course, when PebblePad is enabled for that course. Users are already registered in Banner and Moodle and PebblePad accesses this information to create the user's account.	Collection	s. 26(c)	
Users access PebblePad via SSO and create profile/portfolio and assets (in Pebble+) - includes uploading work product, images, audio, video, text, etc.	Collection Use	s. 26(c) s. 32(a)	
User (students) logs into PebblePad to complete assignments (via ATLAS Workspaces), access online content, obtain information, and utilize tools, services, and features.	Collection Use	s. 26(c) s. 32(a)	
User (instructors) logs into PebblePad to create Workspaces; add student users to Workspaces; create resources; review student content (via ATLAS or directly shared); access online content; utilize tools, services, offerings; provide feedback/assessment; and assign grades.	Collection Use	s. 26(c) s. 32(a)	
User (student) uses PebblePocket app (offline or online) to record assets (including reflections, posts, photos, or video recordings) that will be uploaded/synced to PebblePad account when connected to wifi. PebblePocket app is optionally downloaded to user's personal device. Assets are stored locally on user's device and can be removed by user.	Collection Use	s. 26(c) s. 32(a)	
User (student) grants access to PebblePad portfolio and/or assets to the web or to specific external guest users. External users or public users may provide comments/feedback depending on user's sharing settings.	Use Disclosure Collection	s. 32(a) s. 33(2)(d) s. 26(c)	
PebblePad discloses personal information to third parties to provide services, support, and notifications to users (limited – see #7).	Use Disclosure	s. 32(a) s. 33(2)(d)	
PebblePad sends notifications to user's email according to profile preferences (individual notification or digest) for grades, feedback, comments, assets shared with user, collaborative asset updated, etc.	Use	s. 32(a)	
Users optionally grant temporary access to their PebblePad account for troubleshooting via profile. User provides reason for temporary access; selects Administrator or provides email; and duration of temporary access.	Use	s. 32(a)	

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FIPPA authority or other legal authority**	**Specify any potential risks**
PebblePad discloses assigned numerical grades for any gradable assignment to Moodle gradebook. All other information (comments, feedback, etc.) an instructor has provided to PebblePad remain in PebblePad and are not disclosed.	Disclosure	s. 33(2)(d)	
Student creates an alumni account upon graduation (provides username, personal email) and transfers their information to this account.	Collection Use	s. 26(c) s. 32(a)	
VCC PebblePad Admin deletes inactive accounts as appropriate and PebblePad permanently removes deleted accounts at the end of each annual licence period.	Disposal	s. 31	Potential loss of PI but grades are recorded in Moodle, meeting retention requirements, and students can download coursework.

6. Collection Notice and Consent

6. 1 Collection Notice

If you are collecting personal information directly from an individual the information is about, FIPPA s. 27(2) requires that you provide a collection notice (except in limited circumstances). If your vendor is collecting personal information on behalf of VCC, the vendor must also provide a collection notice. FIPPA requires that you notify the individual of:

- *the legal authority,*
- *purpose(s) and use of their personal information (including any third party disclosures), and*
- *contact information or someone who can answer questions about the collection and use.*

Review the template collection notice below and update as applicable.

Collection notice:

PebblePad, licensed through VCC, collects your personal information under the authority of s. 26(c) of the BC *Freedom of Information and Protection of Privacy Act* (FIPPA). This information will be used to create your PebblePad account, link your account to your VCC Moodle course, and to provide you with access to all PebblePad's services, including creating your portfolio and participating in your courses' Workspaces. Questions about the collection of this information may be directed to eLearning Support at elsupport@vcc.ca

The collection notice will be posted on the Educational Technologies webpage, following the VCC website migration project in 2026. The use of personal information from Moodle/Banner for account creation and linking to Moodle courses is consistent with the purposes of collection for those systems.

6. 2 Consent

If you are obtaining consent for the use or disclosure of personal information (indicated by the FIPPA authorities you used in Question 5), add any consent language here.

N/A

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

No: All data within user accounts and user created-content held within PebblePad is stored in Canada.

s. 15(1)(l)

Some personal data may be transferred of Canada via PebblePad's third-party sub-processors: Canada Sub-processors - August 2025(support requests, business contacts). For data held within PebblePad, the only user-created content that may be transferred outside of Canada temporarily is audio/video content; PebblePad uses the sub-processor Brightcove, Inc. (Republic of Ireland) for the conversion of video content to browser playable formats.

- If no, skip to Part 5.

8. If you answered yes to Question 7: Where are you storing the personal information involved in your initiative?

Be specific about the location where the personal information is stored (e.g. which state(s) or country/countries).

N/A

9. Does your initiative involve sensitive personal information that will be stored outside of Canada?

Sensitive personal information is not defined in FIPPA. Personal information may be considered sensitive depending on the type of information and the context in which it is collected, used, disclosed, or stored. Common sensitive personal information could include: personal health or medical information; financial *information; criminal records; disciplinary or complaint history; unique government issued identifiers (passport number, driver's license, personal health number, SIN); racial or ethnic origins; sexual orientation; religious or philosophical beliefs; etc. Please see the above link for more guidance or consult with VCC's Privacy Office.*

No.

- If no, skip ahead to Part 5

10. If you answered "yes" to Question 9: Is the sensitive personal information being stored outside of Canada only because it is being made available to the public under an enactment that authorizes or requires the information to be made public (FIPPA section 33(2)(f))?

N/A

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section **only if you answered yes to Question 9: you are disclosing sensitive personal information to be stored outside of Canada**. This section will require consultation with a representative from IT Services.

11. Is the sensitive personal information stored by a service provider?

[Answer: Yes or No]

- If yes, fill in the table below (add more rows if necessary) and then go to question 13
- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

12. If you answered "no" to Question 11: Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

This should include reference to the location and method of storing the personal information (e.g. location of data: Atlanta, GA, USA. Method of storing data in Atlanta, GA, USA: e.g. specify that the information is stored in a data storage facility).

[Answer]

13. Does the contract you rely on include privacy-related terms?

[Answer: Yes or No]

- If yes, describe the contractual measures related to your initiative.
  - [Answer]
- Is VCC's Privacy Protection Schedule or Privacy Protection Schedule for Cloud Services appended to the initiative's contract? [Answer: Yes or No]

14. What controls are in place to prevent unauthorized access to sensitive personal information?

Describe technical, security, administrative and/or policy measures that are in place to protect against the unauthorized collection, use, disclosure or storage of sensitive personal information, including preventing or managing access to sensitive personal information. If your initiative uses a cloud-based service provider, also consider controls at each layer: software, platform, and infrastructure.

See Section 2 of the Guidance Document for examples of these measures and consult with IT Services to answer this question.

[Answer]

15. Provide details about how you and will track access to sensitive personal information.

Describe how you will know if the sensitive personal information is accessed, including access by service providers (e.g. logging access to data). Consult with IT Services to answer this question.

[Answer]

16. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence, and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary. See Section 3 of the Guidance Document for examples of privacy risks and risk responses and more guidance for how to complete this table, or see the Guidance on Disclosures Outside of Canada.

Privacy risk	**Impact to individuals (low, medium, high)**	**Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)**	**Level of privacy risk (low, medium, high, considering the impact and likelihood)**	**Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)**	**Is there any outstanding risk? If yes, please describe.**

Outcome of Part 4

The outcome of Part 4 will be a **risk-based decision made by the role designated accountable for the initiative on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 16.

Is the outcome to proceed with the initiative? [Answer: Yes or No]

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5, you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You and/or your vendor need to make sure that the personal information is safely secured in both physical and technical environments.

17. Does your initiative involve digital tools, databases, or information systems?

Yes

- If yes: Are these digital tools, databases, or information systems new to VCC?
  - Yes

17.1 If you answered "yes" to Question 17: Do you or will you have a security assessment to ensure the initiative meets the security requirements of FIPPA s. 30?

Consult with VCC IT Services to complete a security assessment that will ensure that the initiative has reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or disposal of personal information.

Yes: IT Services confirmed on 2025/10/15 that the security assessment was completed.

- If yes, go to question 19. If you have or will complete a security assessment during the development of your initiative, you do not need to answer the question about technical security.

18. What technical and physical security do you have in place to protect personal information?

Describe <u>where the records, whether digital or physical, for your initiative are stored</u> (e.g., on your organization's LAN, on your computer desktop, in a filing cabinet, etc.) and the technical and/or physical security measures in place to protect those records. (Please consult the policies for any software/cloud services/etc. but please do not just copy and paste).

- *<u>Technical security</u> measures include secure passwords, encryption, firewalls, etc.*
- *<u>Physical security</u> measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc.*

IT Services has completed a security assessment for PebblePad. BCNET Master Agreement includes the Privacy Protection Schedule (Schedule 5) and Security Schedule (Schedule 6) for cloud services. PebblePad is ISO 27001 and Cyber Essentials certified.

19. Controlling and tracking access

Please respond to each strategy that describes how you or your vendor limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. To effectively protect privacy, access to personal information should be limited to authorized employees who need the information to do their jobs. Insert your own strategies if needed.

Strategy	
We only allow employees in certain roles access to information:	Yes: For staff, PebblePad uses role-based access controls with restrictive permissions to specific information and staff do not have access to unencrypted client data. PebblePad uses roles with certain permissions for administration within the platform that can be assigned to users (instructors, CTLR admin). This includes high-level administration roles and roles for users, including "Managers" (i.e. for a Workspace in ATLAS – generally instructors)
Employees that need standing or recurring access to personal information must be approved by their managerial lead:	Yes at PebblePad: access is reviewed regularly, including a minimum annual review of access levels or review during any change of job role. Yes at VCC: CTLR is responsible for approving and creating admin accounts.
We use audit logs to see who accesses a file and when:	Yes
Describe any additional controls:	s. 15(1)(l) [redacted]

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6, you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

20. How will you make sure that the personal information is accurate and complete?

FIPPA s. 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete. For example: verifying information with the person it is about prior to recording it.

Users, including students, employees, and guests, are responsible for ensuring the accuracy of the personal information they provide through user content. For students and employees, accounts are created through VCC credentials (information pulled from Banner and Moodle) and those are responsible for ensuring the accuracy of the personal information they provide when registering to VCC or to those systems.

21. Requests for correction

FIPPA s. 29 gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

21.1 Do you have a process in place to correct personal information?

Yes: Users can update their personal information in Banner and/or in Moodle and, as long as the unique identifier linking a user's Moodle and PebblePad information remains the same, any updates will be synched with the corresponding PebblePad account when a user follows a link from Moodle into PebblePad. Users are able to update their user-created content or may request corrections/annotations to specific personal information (e.g. assignments) from the appropriate instructor.

Users (students, employees) can follow regular VCC procedures to update or change personal information including elements like preferred names, upon request to Banner Admin/Registrar's Office or People Services.

21.2 Sometimes it's not possible to correct the personal information. FIPPA s. 29 requires that you make a note on the record about the request for correction if you are not able to correct the record itself. Will you document the request to correct or annotate the record?

Yes

21.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FIPPA s. 29 requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

N/A – VCC does not disclose personal information to a third party in this initiative. Any external disclosure is controlled by the student users.

A student may personally disclose their PebblePad information (sharing assets, linking their portfolio, etc.) to an external assessor (e.g. a workplace mentor); in these cases, the external individual will only see the content that is shared and the student's profile name, and the student user will control this access. The individual user may choose to disclose their personal information via sharing their assets, linking to their portfolio, etc. within PebblePad. Any corrections or updates they make to their personal information will be visible to the external individuals.

22. Does your initiative use personal information to make decisions that directly affect an individual?

Yes: VCC employees may use personal information to make assessments, assign grades, provide learning content or apply educational decisions that directly affect users of PebblePad and to administer related programs and services. Grades assigned to student assignments in PebblePad will be sent back to Moodle.

23. If you answered "yes" to Question 22: Do you have a records retention schedule in place related to personal information used to make a decision?

FIPPA s. 31 requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. Please consult the VCC Records Retention Schedule to assist you in answering this question.

Yes: Student assignments and examinations (TE-400) may be destroyed after two years. Grading in PebblePad is synched with VCC's Moodle gradebook. Grades are maintained for 7 years (TE-600).

Instructors should remind students that they should ensure that they retain a copy of their assignments if needed. Students can download content from PebblePad typically as a non-editable PDF.

PebblePad data is held for the lifetime of an account. Accounts remain active based on use of PebblePad; user accounts may become inactive when a student or employee has not frequently accessed the account.

VCC is responsible for deleting any inactive user accounts from the PebblePad platform. s. 15(1)(l), s. 21(1) [redacted]

In the case of an organisation discontinuing their PebblePad licence, all associated account and user data is purged 150 days after the licence expiry date.

PART 7: PERSONAL INFORMATION BANKS

24. Will your initiative result in a personal information bank?

A personal information bank is a collection of personal information that is organized and retrievable by the name of the individual or an identifying number, symbol or other identifier.

Yes (see Personal Information Directory)

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

25. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible risk	**Response / mitigation strategies**
Unauthorized employees/service providers could access the personal information in the system and use or disclose it for personal purposes.	VCC employees must follow VCC conduct and FIPPA policies Use of SSO/password-protected access, permissions restrictions, and other information security measures. Legal agreement with service provider (via BCNET), including privacy provisions. (BCNET PIA)
PebblePad/AWS/Microsoft Azure Security Breach	PebblePad breach protocols are in place to reduce risks to VCC's data in the event of a security breach. Data is always encrypted during transmission or while being processed by PebblePad. Per contractual obligations and privacy provisions, PebblePad must promptly report any privacy breaches. Under BCNET member specific contracts, PebblePad is responsible for subcontractors privacy data flow downs. (BCNET PIA)
Creation of new personal information (data matching)	Governed by contractual obligations & PPS PebblePad is only permitted to access and use data pursuant to the PebblePad-VCC contract for the service. (BCNET PIA)
Unauthorized collection, disclosure or access to personal information, or unauthorized retention, by third parties (e.g. AWS, Microsoft Azure)	Per contractual obligations/ conditions/terms/agreement and third party subcontractor requirements (PPS, CSS). Under BCNET member specific contracts, PebblePad is responsible for subcontractors privacy data flow downs.(BCNET PIA)
Unauthorized retention of personal information by PebblePad	Per contractual obligations, conditions, terms and agreement with BCNET & its members (PPS, CSS). PebblePad is only permitted to retain data pursuant to the specific contract for the service. (BCNET PIA)
Users unintentionally disclose personal information via sharing "assets" within portfolio via live links.	All individuals with access to a live link will continue to see all updates unless the user removes the share, including items linked to the item shared. Users (students) must ensure that they are

Possible risk	Response / mitigation strategies
	appropriately sharing their assets. Shares cannot be removed for shares with ATLAS once the assessment process has begun.
Users may collect third party personal information through the content they upload to the PebblePad system (e.g. experience recordings; photos or videos; reflections on experiential learning that involve other individuals; questionnaires)	Guidance should be provided to all users to minimize the amount of third-party personal information provided to PebblePad, especially without others' consent (e.g. not recording anything that could identify other individual; speaking about personal experience but not others' identifiable experiences).
Users provide PebblePad with access to third-party drives (e.g. OneDrive, Google Drive)	Linking is optional and PebblePad will pull information from the drive into PebblePad and make it available to the user but it will not be amended or stored in the software, and the user may disable the link at any time. Users (students) should not connect with Google Drive or any third-party drive not supported by VCC.

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to the Privacy Office for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Recommended for approval.

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer	Caralee Maloney	Caralee Maloney Digitally signed by Caralee Maloney Date: 2025.11.27 11:47:04 -08'00'	November 27, 2025

Program Area Signatures

The PIA must be signed by a role that is able to hold accountability for a PIA, proportionate to the sensitivity of personal information and/or the risks of the initiative. This signature confirms that this PIA accurately documents data elements and information flow at the time of signing. If there are any changes to the overall initiative, including the way personal information is collected, used, stored, or disclosed, the program area will contact Privacy and, if necessary, complete a PIA update.

Program Area Comments:

Role	Name/Position	Electronic signature	Date signed
Role designated accountable for the initiative	Andrew Dunn, Manager Online Learning	Andrew Dunn Digitally signed by Andrew Dunn Date: 2025.12.03 14:24:47 -08'00'	December 3, 2025
Contact Responsible for Systems Maintenance and/or Security	Norman Chang Director IT	Norman Chang Digitally signed by Norman Chang Date: 2025.12.03 12:23:27 -08'00'	December 3, 2025