



Office of the Victorian
Information Commissioner

Privacy Impact Assessment

OVIC Learning Management System

Part 1 – Program background and details

Program	OVIC Learning Management System
Drafted By	Policy Team
Responsible Team	Communication and Education Team
Assessment Date	July 2023

Description and benefit of the learning management system

A mandate of the Office of the Victorian Information Commissioner (**OVIC**) is to deliver proactive and integrated information access, privacy and security leadership in Victoria, particularly by driving the cultural shifts necessary to improve the way government manages and provides access to information.

A strategy to enable OVIC to influence cultural change in the public sector is to provide a robust and diverse training program across each functional area of OVIC. An element of this training program is providing public sector organisations with an online training platform. Online training enables OVIC to reach a wider audience than traditional face-to-face training by:

- allowing users to access free training anytime; and
- making training available and accessible to public sector organisations located regionally.

OVIC utilises an online Learning Management System (**LMS**) called Learnbook. Learnbook is distributed by eCreators. It can be accessed via a link on the online learning page of OVIC's website. The platform currently provides free educational courses on privacy and freedom of information.

Collection and use of personal information

Individuals need to create an account to use the LMS. Individuals may use their account to access the training modules, and to receive a certificate with their name on it after completing a course. Users may also be notified by email about updates to training modules and the LMS.

When creating an account, users are required to provide the following mandatory information:

- First name and Last name
- Email Address
- Agency/Organisation

The following optional fields are also present:

- City/Town
- Country

The optional fields cannot be disabled.

When using the LMS, the IP address of users is collected, as well as live log data of the user showing the date and time, name of user, IP address and the 'event'. An 'event' is an interaction with the LMS by a user, such as opening a section of a course, completing a course, navigating to the dashboard, viewing their user

profile. The Communications and Education team do not use live log data to generate reports. The live log data is used by eCreators IT support, to locate and remedy any technical and accessibility issues experienced by users.

Parties involved including contracted service providers (CSPs)

The LMS currently uses Learnbook, which is a modified version of the free and open source software, LMS Moodle. Learnbook is distributed by eCreators. OVIC entered into a contract with eCreators for the right to use Learnbook. The LMS is separate to OVIC's website and is hosted by Amazon Web Services (**AWS**).

eCreators is owned by OpenLMS, which is a company within the Learning Technologies Group of companies. LMS user registration information, live log data and IP addresses can be accessed by eCreators using the LMS administration account. More information can be found in eCreators [privacy policy](#). Moodle Pty Ltd creates software and services for education processes. They created an LMS called Moodle, making it free and open source under the GNU General Public License. This means that anyone can modify, distribute, and sell the LMS Moodle with minimal restrictions. Learnbook is a modified version of the LMS Moodle. Moodle Pty Ltd has no direct involvement in this project.

AWS is an American company that offers cloud services such as hosting, computing, and storage. The LMS and associated personal information is stored in an AWS data centre located in Sydney. The data cannot be moved from that location without OVIC's consent. AWS has a [privacy policy](#) and a [white paper about using AWS services in the context of Australian privacy legislation](#).

Interactive third-party plugins such as Google, Youtube, Dropbox, Webex, Paypal, Jabber and Zoom have been disabled on the LMS. Based on information provided by eCreators, third party plugins active on the LMS enable functionality only. They do not collect information. The plugins used on OVIC's website are the same – they are for functionality only and do not collect information. The LMS web address has been scanned using [Blacklight](#), a real-time website privacy inspector. The results did not find any third party tracking or concerning privacy practices present on the LMS.

Scope of this privacy impact assessment

The scope of this PIA covers the way personal information is collected, stored and handled through the LMS. This includes information collected from individuals when they interact with the LMS (for example, when registering an account), as well as the information collected automatically from users when visiting the LMS (live log data and IP addresses).

This PIA only relates to personal information collected by OVIC, eCreators and AWS.

This PIA does not include an analysis by OVIC of each individual plugin that enables functionality on the LMS. The PIA relies on information provided by eCreators, and the Blacklight results, to conclude that no third-party plugins collect information from the LMS.

Legal authority

The objects of the *Privacy and Data Protection Act 2014 (PDP Act)* outlined in section 5 include:

- to promote awareness of responsible personal information handling practices.
- to promote the responsible and transparent handling of personal information in the public sector.
- to promote responsible data security practices in the public sector.

The information privacy functions of the Information Commissioner and Privacy and Data Protection Deputy Commissioner as set out in section 8C(2) include:

- to promote understanding and acceptance of the Information Privacy Principles and of the objects of those Principles.

The information security functions of the Information Commissioner and Privacy and Data Protection Commissioner as set out in section 8D(1) include:

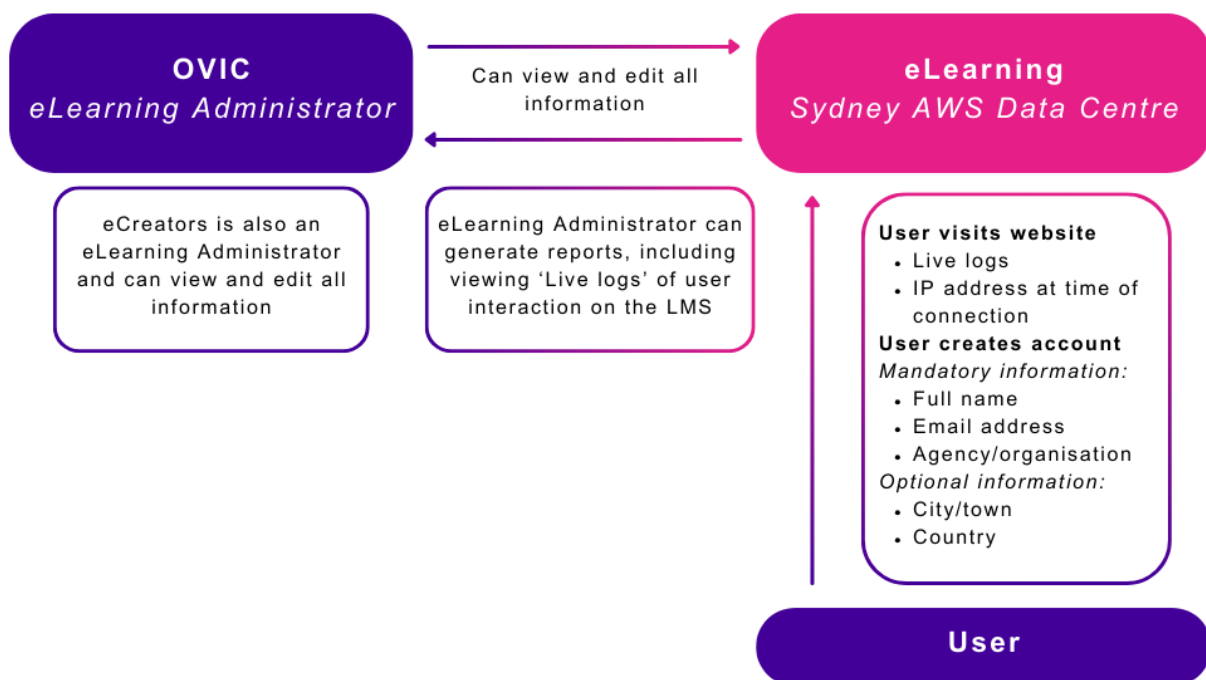
- to promote the uptake of protective data security standards by the public sector.

Section 6I(2) of the *Freedom of Information Act 1982 (FOI Act)* includes the following functions:

- to promote understanding and acceptance of the FOI Act and the object of the Act.
- to provide advice, education and guidance in relation to compliance with professional standards.
- to provide advice, education and guidance in relation to the Information Commissioner’s functions.

It is important for the educational functions detailed above to be made available in various formats including online. The LMS is essential for dissemination of education to government agencies. Personal information collected through the LMS is necessary to fulfil OVIC’s functions as set out in the PDP Act and the FOI Act.

Figure 1. Information flow diagram



Part 2 – Privacy analysis

This part identifies the privacy elements and risks of the program. The PIA Guide provides guidance on responding to the questions. The right column indicates the relevant section of the PIA Guide. Some questions may not be relevant or applicable. The response should be noted as N/A where this occurs.

Identify the information elements

	Question	Response	Guide
1	<p>Does the program involve personal information?</p> <p><i>List each piece of personal information that is involved in the program.</i></p>	<p>Yes. Individuals need to create an account to use the LMS. When registering an account, individuals are required to provide:</p> <ul style="list-style-type: none"> • First name • Last name • Email address • Agency/Organisation <p>The registration page also includes the following optional fields that cannot be disabled:</p> <ul style="list-style-type: none"> • City/Town • Country <p>When using the LMS, live log data is collected about a user's interaction with the LMS including date and time of log in, course access and course completion, the person's user account name, most recent IP address and each click navigation of the LMS.</p> <p>Information provided directly by users, IP address and live log data is collected by OVIC, eCreators and AWS. This information can only be accessed by OVIC and eCreators using the LMS administration account.</p>	<p><i>Para No. 6.2 – 6.5</i></p> <p><i>Page No. 16 – 17</i></p>
2	<p>Does the program involve other information that has the potential to identify individuals?</p> <p><i>This may include information that does not appear to be personal information at first glance, but which could identify individuals based on the context of the project or how the program uses the information.</i></p> <p><i>Describe this other information and explain how it could potentially identify individuals within the context of your program.</i></p>	<p>No. The LMS does not involve other information that has the potential to identify individuals.</p>	<p><i>Para No. 6.6</i></p> <p><i>Page No. 17</i></p>
3	<p>Does the program involve sensitive information (as defined under Schedule 1 of the PDP Act)?</p> <p><i>Describe the type(s) of sensitive information that is involved in the program (if any), and how the collection or use of the sensitive information is authorised either by the PDP Act or other legislation.</i></p>	<p>No. Individuals are not required to provide sensitive information when engaging with OVIC via the LMS.</p>	<p><i>Para No. 6.7 – 6.9, 7.4</i></p> <p><i>Page No. 17 – 18, 20</i></p>

4	<p>Does the program involve health information?</p> <p><i>If the answer is yes, please refer to the Health Records Act 2001 or consult with the Health Complaints Commissioner in relation to health information (and where applicable, the Office of the Australian Information Commissioner).</i></p>	<p>No. Individuals are not required to provide health information when engaging with OVIC via the LMS.</p>	<p><i>Para No. 6.10</i></p> <p><i>Page No. 18</i></p>
5	<p>Does the program involve information that has previously been de-identified?</p> <p><i>Describe the type(s) of de-identified information that is involved in the program (if any), and the potential for re-identification.</i></p>	<p>No. The program does not involve information that has previously been de-identified.</p>	<p><i>Para No. 6.13 – 6.18</i></p> <p><i>Page No. 19</i></p>

Collection of personal information

6	<p>Is all the personal information collected necessary for the program?</p> <p><i>Explain why all the information collected is necessary for your program.</i></p>	<p>No. The optional fields and Agency/Organisation field on the registration page are not necessary for the program. However, due to technical constraints of the LMS, these fields cannot be disabled.</p> <p>The IP address and live logs are necessary for a short time to provide technical support to users who may encounter an issue with using the LMS.</p>	<p><i>Para No. 7.2 – 7.3</i></p> <p><i>Page No. 20</i></p>
---	---	---	--

Privacy risk: If some personal information is not necessary for the program, consider whether there is a risk of overcollection.

7	<p>Do you need to collect information that identifies an individual for the purposes of the program, or can individuals remain anonymous?</p>	<p>Registering an account on the LMS: Individuals cannot remain anonymous. Individuals receive a certificate with their name on it after completing a course. The name is based on the name the person used when registering an account.</p> <p>Live log data: Individuals cannot remain anonymous. Live log data needs to be linked back to the user for a short time, to provide the user with technical support. The live logs identify the individual because of the requirement to use the individual's name to register a user account.</p>	<p><i>Para No. 7.5</i></p> <p><i>Page No. 21</i></p>
8	<p>If individuals can remain anonymous, will you be collecting indirect identifiers, such as demographic information?</p>	<p>No.</p>	<p><i>Para No. 6.3 – 6.4</i></p> <p><i>Page No. 17</i></p>

Method and notice of collection

9	<p>How will the personal information be collected?</p> <p><i>Describe the means by which the information will be collected. If personal information is collected via a third party platform, explain whether the platform will also be collecting that information</i></p>	<p>Personal information is collected by OVIC, eCreators and Amazon Web Services when individuals register an account on the LMS, use the LMS and complete an LMS course.</p>	<p><i>Para No. 7.7 – 7.8</i></p> <p><i>Page No. 21</i></p>
---	---	--	--

Privacy risk: Consider whether your method of collection is fair and not unreasonably intrusive.

10	<p>Is the personal information collected directly from the individual?</p>	<p>Personal information is collected directly from the individual when they register an account on the LMS. The IP address of the user and user live log data is collected whenever they login to and use the LMS.</p>	<p>Para No. 7.9</p> <p>Page No. 21</p>
11	<p>Will the individual be notified about the collection of their personal information?</p> <p><i>Describe the steps taken to provide notice to the individual OR explain why notice will not be provided to the individual. Include a link or attach collection notices where appropriate.</i></p>	<p>Information about the collection of personal information on the LMS is included in OVIC's online collection notice and website privacy statement.</p> <p>Links to the collection notice and website privacy statement are provided at the following points along the user journey to accessing and using LMS:</p> <ul style="list-style-type: none"> • on the online learning page of OVIC's website, just above the link that takes individuals to the external website of the LMS; • on the welcome login page of the LMS (this is the page that also includes the link to 'sign up' to the LMS); • in the registration email sent to individuals, after they first create an account on the LMS; and • in the left-hand side menu bar, when a user is logged into the LMS. 	<p>Para No. 7.13 – 7.16</p> <p>Page No. 22</p>
12	<p>Will any personal information about the individual be collected indirectly from another source?</p> <p><i>Describe how and from which other sources the personal information will be collected.</i></p>	<p>No. Personal information is not collected indirectly from another source.</p>	<p>Para No. 7.10 – 7.11</p> <p>Page No. 21 – 22</p>
<p>Privacy risk: If you are collecting personal information indirectly, consider whether there is a risk of the information being inaccurate, out of date or incomplete. Consider the impact on individuals if they are not made aware that their information is being collected from another source.</p>			
13	<p>Will the individual be notified that their personal information has been collected from another source?</p> <p><i>Describe the steps taken to provide notice to the individual OR explain why notice will not be provided to the individual. Include a link or attach collection notices where appropriate.</i></p>	<p>N/A</p>	<p>Para No. 7.15</p> <p>Page No. 22</p>

Unique identifiers

<p>14</p>	<p>Will the program assign a unique identifier or collect a unique identifier assigned by another organisation to adopt as your organisation's own?</p> <p><i>Describe the unique identifier, the purpose for assigning or collecting it, and how this is authorised by either the PDP Act or other legislation.</i></p>	<p>No. A unique identifier is not assigned or collected when an individual interacts with the LMS.</p>	<p><i>Para No. 7.18 – 7.19</i></p> <p><i>Page No. 23</i></p>
<p>15</p>	<p>Does the program require an individual to provide a unique identifier?</p> <p><i>Explain why or how the provision of a unique identifier is necessary for the program.</i></p>	<p>No. Individuals are not required to provide a unique identifier to engage with OVIC via the LMS.</p>	<p><i>Para No. 7.20 – 7.21</i></p> <p><i>Page No. 23</i></p>

Quality of personal information

<p>16</p>	<p>What steps will you take to ensure the personal information collected is accurate, complete, and up to date?</p>	<p>All personal information collected via the LMS is collected directly from the individual and is therefore assumed to be accurate, complete and up to date at the time of collection.</p> <p>When an individual registers an account on the LMS, a confirmation email is sent to the email address provided during the sign up process to confirm it is the right email address and provide mechanisms for the individual to update their details or opt out of the mailing list if they wish to.</p>	<p><i>Para No. 9.16 – 9.18</i></p> <p><i>Page No. 27 – 28</i></p>
-----------	--	---	---

Privacy risk: If there are inadequate or no steps taken, consider whether there is a risk that the information will be inaccurate, incomplete or out of date.

Security of personal information

<p>17</p>	<p>Are there security measures in place (existing or intended) to protect the personal information collected and used for this program?</p> <p><i>List the policies, procedures, or controls that your organisation implements to protect personal information. Please indicate how these measures will be governed. Include links or attachments where appropriate</i></p>	<p>Yes.</p> <p>Refer to Ecreators Security Risk Assessment [D22/22827] and Briefing Note [D23/1986] for detailed security risks, controls and mitigation strategies.</p> <p>OVIC conducts OVIC website penetration test but it does not test subnets.</p>	<p><i>Para No. 8.2 – 8.9</i></p> <p><i>Page No. 23 – 25</i></p>
<p>18</p>	<p>Where and how will personal information be stored?</p> <p><i>Describe the format in which the personal information will be stored (e.g. electronic, hard copy etc.) and where it will be stored (e.g. internally, external provider, cloud, third party platform etc.)</i></p>	<p>All personal information collected through the LMS is stored on Amazon Web Services data centre in Sydney.</p>	<p><i>Para No. 8.2 – 8.9</i></p> <p><i>Page No. 23 – 25</i></p>

<p>19</p>	<p>Who will have access to the personal information?</p> <p><i>Describe the positions that will have access how access is gained or controlled, and whether it is logged.</i></p>	<p>The following have access to personal information collected through the LMS:</p> <ul style="list-style-type: none"> • OVIC Communications and Education Team • Other OVIC staff (for example, IT and the staff preparing the PIA and SRA); • eCreators staff with login access to the LMS backend. 	<p>Para No. 8.2 – 8.9</p> <p>Page No. 23 – 25</p>
<p>20</p>	<p>Have you completed a separate security risk assessment?</p> <p><i>If so, please refer to or attach a copy of the assessment to this PIA. If not, OVIC suggests you complete a security risk assessment.</i></p>	<p>Yes. Please refer to the Elearning website Security Risk Assessment [D22/22827].</p>	<p>Para No. 8.10 – 8.11</p> <p>Page No. 25</p>

Privacy risk: If there are inadequate or no security measures in place, consider whether there is a risk that the information will not be properly protected, leading to loss, misuse, or unauthorised access, modification or disclosure.

Primary and additional uses and disclosures of personal information

<p>21</p>	<p>Is the personal information (including any sensitive information) involved in this program used or disclosed for the main or primary purpose for which it was collected?</p> <p><i>Describe what personal information will be used or disclosed, and for what purposes.</i></p>	<p>Yes.</p> <p>Personal information is used for registering an account on the LMS, to access a user’s history of course completion to generate updated certificates of completion, and to access live logs to assist in resolving technical issues a user may experience when using the LMS.</p>	<p>Para No. 9.2</p> <p>Page No. 25</p>
<p>22</p>	<p>Does the program use or disclose personal information (including sensitive information) for a new or additional purpose other than the original purpose of collection?</p> <p><i>Describe the new/additional purpose for the use or disclosure of the information and explain how it is authorised, by either the PDP Act or other legislation. If relying on IPP 2.1(a), explain how the secondary use or disclosure is related to the primary purpose of collection.</i></p>	<p>Yes. The information collected to register an account may be used to notify users by email about updates to the training modules and LMS. This secondary purpose is related to the primary purpose of collecting the information to enable the individual to complete training modules on the LMS. An individual would reasonably expect their information to be used for this secondary purpose.</p>	<p>Para No. 9.3 – 9.4</p> <p>Page No. 26</p>

Privacy risk: If relying on IPP 2.1(a) to use personal information for a secondary purpose, consider whether individuals would reasonably expect their information to be used for that secondary purpose. If relying on IPP 2.1(b) to use personal information for a secondary purpose, ensure the individual’s consent is meaningful.

<p>23</p>	<p>Will the individual be notified of the additional use(s) of their personal information?</p> <p><i>Explain how the individual will be given notice of the secondary use(s) of their information, or why notice of the secondary use will not be provided.</i></p>	<p>Yes. The secondary purpose is stated in the collection notice that is linked to users:</p> <ul style="list-style-type: none"> • on the online learning page of OVIC’s website, just above the link that takes individuals to the external website of the LMS; • on the welcome login page of the LMS (this is the page that also includes the link to 	<p>Para No. 9.4</p> <p>Page No. 26</p>
-----------	--	--	--

		<p>‘sign up’ to the LMS);</p> <ul style="list-style-type: none"> in the registration email sent to individuals, after they first create an account on the LMS; and in the permanent left-hand side menu bar, when a user is logged into the LMS. 	
--	--	--	--

Transfer and sharing of personal information

24	<p>Will any personal information be shared outside of your organisation?</p> <p><i>Describe:</i></p> <ul style="list-style-type: none"> what information will be shared; with whom the information will be shared; the frequency of the disclosure; how the information will be shared; and how the disclosure is authorised by either the PDP Act or other legislation. <p><i>Identify whether any information sharing agreements are or will be in place.</i></p>	<p>Personal information collected on the LMS is collected and stored directly in an AWS data centre in Sydney. OVIC and eCreators can access personal information collected on the LMS through the LMS administrator account. The personal information is not shared unless required by law.</p>	<p><i>Para No. 9.6 – 9.7</i></p> <p><i>Page No. 26</i></p>
25	<p>Will any personal information be transferred outside Victoria?</p> <p><i>Describe what information will be transferred, to whom the information will be transferred, in which jurisdiction the information will be stored, and how the information will be transferred. Explain how the transfer is authorised by either the PDP Act or other legislation.</i></p>	<p>Personal information collected on the LMS is collected and stored directly in an AWS data centre in Sydney. There is no transfer of personal information from OVIC to AWS. AWS cannot transfer data to a different jurisdiction without OVIC’s consent.</p> <p>AWS is subject to the Australian Privacy Principles in the <i>Privacy Act 1988</i> (Cth). The use of AWS in Australia is summarised in an AWS document ‘Using AWS in the Context of Australian Privacy Considerations’.</p>	<p><i>Para No. 9.8 – 9.9</i></p> <p><i>Page No. 26</i></p>

Other considerations relating to use and disclosure

26	<p>Does the program use or disclose a unique identifier assigned by another organisation?</p> <p><i>Describe the unique identifier and how it will be used or disclosed, and whether this is authorised by either the PDP Act or other legislation.</i></p>	No.	<p><i>Para No. 9.10 – 9.11</i></p> <p><i>Page No. 27</i></p>
27	<p>Will any data matching occur as part of this program? This includes matching datasets within the program, or matching to other datasets external to the program.</p> <p><i>If so, explain the purpose for the data matching, what personal information will be matched and what other datasets it will be matched with, and what the combined dataset will be used for.</i></p>	No.	<p><i>Para No. 9.13 – 9.14</i></p> <p><i>Page No. 27</i></p>
28	<p>Will any personal information be de-</p>	No.	<p><i>Para No. 6.14 – 6.18</i></p>

	<p>identified as part of the program?</p> <p><i>Describe the purpose for de-identifying personal information for the program, the method of de-identification, how the de-identified information will be used, and the potential for re-identification.</i></p>		<p>Page No. 19</p>
<p>Privacy risk: If personal information is de-identified, consider whether there is a risk that the information can be re-identified. For example, de-identified information may be re-identifiable when matched to other information, or because of the way the de-identified information is used in the context of this program.</p>			
<p>29</p>	<p>What will be done to ensure the ongoing accuracy, completeness, and currency of the personal information?</p> <p><i>Describe the steps that will be taken, or the measures that are in place, to ensure the ongoing integrity of the information.</i></p>	<p>Personal information collected to register an account on the LMS is collected directly from the individual and is therefore assumed accurate, complete and up to date.</p>	<p>Para No. 9.16 – 9.18</p> <p>Page No. 27 – 28</p>

Management of personal information

<p>30</p>	<p>Is there a document available to the public that sets out your organisation's policies for the management of personal information, such as a privacy policy?</p> <p><i>Identify the document(s) and provide a link where available or include as an attachment to this PIA.</i></p>	<p>Yes. OVIC's privacy policy provides general details on how personal information is handled by OVIC.</p> <p>The website privacy statement provides details regarding third party collection.</p> <p>A collection notice is included:</p> <ul style="list-style-type: none"> on the online learning page of OVIC's website, just above the link that takes individuals to the external website of the LMS; on the welcome login page of the LMS (this is the page that also includes the link to 'sign up' to the LMS); in the registration email sent to individuals, after they first create an account on the LMS; and in the permanent left-hand side menu bar, when a user is logged into the LMS. 	<p>Para No. 10.2, 10.5</p> <p>Page No. 28</p>
<p>31</p>	<p>Will the document be updated to reflect the new collection or use of personal information for the purposes of this program?</p> <p><i>If not, explain why.</i></p>	<p>These documents are updated as and when required.</p>	<p>Para No. 10.3</p> <p>Page No. 28</p>
<p>32</p>	<p>Is there a way for a person to find out the types of personal information your organisation holds about them? Can you tell them the purposes for which it is held, and how your organisation collects, holds, uses and discloses that information?</p> <p><i>Describe the steps and provide links where relevant.</i></p>	<p>Individuals can contact enquiries@ovic.vic.gov.au or OVIC's privacy officer to find out the personal information OVIC holds about them, the purposes for which it is held and how OVIC manages that information.</p> <p>OVIC's collection notice, website privacy statement and privacy policy outlines these matters.</p>	<p>Para No. 10.4 – 10.5</p> <p>Page No. 28</p>

Access and correction of personal information

33	<p>How can individuals request access to, or correct their personal information?</p> <p><i>Identify the avenues available for individuals to request access to or correction of their personal information, and who is responsible for handling such requests.</i></p>	<p>Individuals who wish to access or correct the personal information provided via the LMS can contact OVIC via enquiries@ovic.vic.gov.au.</p> <p>The training@ovic.vic.gov.au email address is also provided on the landing page of the LMS.</p>	<p><i>Para No. 10.6 – 10.7</i></p> <p><i>Page No. 29</i></p>
----	---	--	--

Privacy risk: If engaging third parties such as contracted service providers, consider whether there are arrangements in place to allow access and correction of personal information held by third parties. If not, there may be a risk that individuals cannot access or correct their personal information.

Retention and disposal of personal information

34	<p>How long will the personal information be kept for?</p> <p><i>Describe any relevant retention and disposal schedules or policies, including those issued by the Keeper of Public Records or those in other legislation.</i></p>	<p>The RDA for records of the Information Regulation Function (PROS 10/16) applies to the development of the content of training programs and the delivery and review of training programs through the LMS. Under PROS 10/16, point 3.1.2, LMS user accounts should be deleted if they have not been accessed for 7 years.</p> <p>Under point 3.1.3, feedback provided by users upon completion of a course should be destroyed 2 years after course completion.</p> <p>The RDA for Records of Common Administrative Functions (PROS 07/01 VAR 7) applies to live log data. Under 19.5.2, this data can be destroyed after OVIC's requirements have ceased. As the live logs are only used to provide IT support to users, this data should be deleted after 30 days. This is a conservative estimate of the live log history that may need to be accessed to resolve an IT issue. Usually, support is required for events occurring same day or same week. Retaining the data for longer than 30 days is unnecessary.</p> <p>Individuals may also request that their LMS account and its associated personal information be deleted by contacting OVIC.</p>	<p><i>Para No. 11.2 – 11.3</i></p> <p><i>Page No. 29 – 30</i></p>
35	<p>How will personal information be destroyed once it is no longer required?</p> <p><i>Describe the method of destruction and explain how that method is secure.</i></p>	<p>Personal information provided for elearning on the LMS will be deleted from the eCreator's Learnbook platform in accordance with the relevant RDA.</p> <p>Recommendation: <i>Comms team develop an internal procedure to govern the ongoing deletion of accounts, feedback and live logs in accordance with the relevant RDA.</i></p>	<p><i>Para No. 11.4</i></p> <p><i>Page No. 30</i></p>

36	<p>As an alternative to destroying personal information, will any personal information be de-identified once it is no longer required?</p> <p><i>Describe the method of de-identification that will be used and the purposes to which the de-identified information will be put.</i></p>	No.	<p><i>Para No.</i> 11.6 – 11.7</p> <p><i>Page No.</i> 30</p>
<p>Privacy risk: If de-identifying personal information once it is no longer required, consider whether there is a risk that the information can be re-identified.</p>			
37	<p>If applicable, what will happen to personal information held by third parties (such as contracted service providers, cloud storage, third party platforms etc.)?</p> <p><i>Describe any arrangements (for example, any contractual provisions) in relation to third parties' obligations to retain and dispose of personal information.</i></p>	It is not known what the data destruction policies are of eCreators under the current contract. However, the Open LMS SaaS Information Security Overview states clients are given copies of their database and files on termination of the contract and that Open LMS securely deletes all data. This security policy will apply when OVIC enters into a contract with Open LMS on or before July 2023).	<p><i>Para No.</i> 11.9 – 11.10</p> <p><i>Page No.</i> 30 – 31</p>
<p>Privacy risk: If there are no arrangements in place relating to third parties' retention and disposal of personal information, consider whether there is a risk that personal information will be held indefinitely.</p>			

Other considerations

38	<p>Who can individuals complain to if they have concerns about the handling of their personal information?</p> <p><i>Identify the avenues (internal and external) for making a privacy complaint, including who is responsible for complaint handling.</i></p>	<p>Individuals can contact OVIC's privacy officer if they have concerns about the handling of their personal information.</p> <p>Email: privacy@ovic.vic.gov.au Phone: 1300 006 842 Post: PO Box 24272, Melbourne VIC 3001</p>	<p><i>Para No.</i> 12.2 – 12.4</p> <p><i>Page No.</i> 31</p>
39	<p>Does your organisation have a data breach response plan in place?</p> <p><i>If so, describe at a high level the steps that your organisation will take in the event of a data breach.</i></p>	<p>Yes. OVIC has a data breach response plan in its Business Continuity plan.</p> <p>OVIC has a security handbook that contains a security incident management framework and an incident reporting section. It states that any breaches of privacy relating to personal information provided by or collected on behalf of OVIC needs to be reported to the privacy officer.</p>	<p><i>Para No.</i> 12.5 – 12.6</p> <p><i>Page No.</i> 31 – 32</p>
40	<p>Will any training be provided to staff to ensure the appropriate collection and handling of the personal information collected for this program?</p> <p><i>Describe the type of training staff will receive.</i></p>	<p>There is no specific training provided to staff who have access to the personal information collected via the LMS.</p> <p>Recommendation: <i>The Executive should select an individual within the Comms and Education team to be the 'LMS champion'. This person should receive training in the editing and use of Learnbook, including running reports, using the LMS backend functions and destroying personal information when no longer required.</i></p>	<p><i>Para No.</i> 12.7</p> <p><i>Page No.</i> 32</p>

41	<p>Will the program be evaluated against its objectives?</p> <p><i>Describe who will evaluate the program, at what point in the program evaluation will occur, and how often.</i></p>	<p>Yes. The Communications and Education Team report usage and satisfaction data on a monthly basis as part of BP3 reporting. An evaluation framework will also be developed for the training and education program incorporating the eLearning component of the program.</p>	<p><i>Para No. 12.8</i></p> <p><i>Page No. 32</i></p>
42	<p>Does the program comply with your organisation's other information handling or information management policies?</p>	<p>Yes.</p>	<p><i>Para No. 12.9</i></p> <p><i>Page No. 32</i></p>
43	<p>Will this PIA be published?</p>	<p>Yes.</p>	<p><i>Page No. 7</i></p>
44	<p>Are there any other broader privacy considerations associated with this program?</p>	<p>No.</p>	<p><i>Para No. 12.10</i></p> <p><i>Page No. 32</i></p>
45	<p>Has the organisation's privacy officer been consulted?</p> <p><i>The organisation's privacy officer should be consulted.</i></p>	<p>Yes.</p>	<p><i>Page No. 6</i></p>

Part 3 – Privacy risk assessment

This part lists any privacy risks that have been identified as part of the analysis in Part 2. Refer to sections 13 – 16 in Part 3 of the PIA Guide (pages 33 – 35) for guidance on completing the risk assessment table.

<p>Were any privacy risks identified in the privacy analysis completed in Part 2 of this PIA?</p>	<p><input checked="" type="checkbox"/> Yes</p> <p>Enter each privacy risk in the risk assessment table below</p>	<p><input type="checkbox"/> No</p> <p>Proceed to Part 4 of this PIA.</p>
--	--	--

	Description of risk	Consequence rating	Likelihood rating	Overall risk rating	Accept	Risk management strategy	Residual consequence rating	Residual likelihood rating	Residual risk rating	Owner
R1	<p>LMS The risk of unauthorised and unlawful collection of personal information.</p> <p>Caused by fields being present during the account creation process for individuals to enter (optionally) their city/town, country, and (mandatorily) their agency/organisation, that are not used for any LMS function.</p> <p>Resulting in legal/regulatory non-compliance with IPP 1 (collection) and dissatisfaction from stakeholders.</p>	Insignificant	Almost Certain	Medium (5)	Yes	<p>Due to technical limitations of the eCreator’s Learnbook platform, these fields cannot be disabled.</p> <p>This risk cannot be mitigated and must be accepted.</p>	Insignificant	Almost Certain	Medium (5)	Communications and Education Team
R2	<p>LMS The risk of unauthorised and unlawful retention of unneeded personal information.</p> <p>Caused by PROS 10/16 RDA 3.1.2 indicating that LMS accounts should be deleted after 7 years of non-use and RDA 3.1.3 indicating that feedback about LMS courses should be deleted 2 years after</p>	Moderate	Almost Certain	Very High(15)	No	Implement a procedure to delete accounts that have not been used for seven or more years, delete user feedback 2 years after it was provided, and Live Logs deleted after 30 days.	Very Unlikely	Minor	Low(1)	Communications and Education team

	<p>delivery; and PROS 07/01 VAR 7 indicating that live log data should be deleted after agency's requirement's cease. However, there is currently no process in place to comply with these requirements.</p> <p>Resulting in legal/regulatory non-compliance with PROS 10/16, PROS 07/01 and IPP 4.2, and dissatisfaction from stakeholders.</p>									
R3	<p>LMS The risk of unauthorised collection and retention of unneeded personal information.</p> <p>Caused by Live Logs being enabled in the backend administration access to the LMS, which logs the date and time of every event (click) by a user logged in to the LMS, and their name and IP address at the time of the event.</p> <p>Resulting in legal/regulatory non-compliance with IPP 1, reputational damage, dissatisfaction from stakeholders and loss of confidence/trust.</p>	Moderate	Almost Certain	Very High (15)	No	<p>The Live Log data links to the name recorded by an individual when they registered an account.</p> <p>Due to technical limitations of the eCreator's Learnbook platform, the Live Log data cannot be configured to de-identify individuals. As a result, the Live Logs record identifiable movements of the user on the LMS.</p> <p>To mitigate this risk, Live Log data should only be stored for the minimum time required. The Communications and Education team should implement a procedure to ensure Live Log data is deleted every 30 days.</p>	Unlikely	Minor	Low(4)	Communications and Education Team
R4	<p>LMS The risk of unauthorised disclosure and transfer of personal information to third parties.</p> <p>Caused by third party plug-ins collecting personal information.</p> <p>Resulting in non-compliance with IPP 2 and IPP 9, reputational damage and loss</p>	Minor	Unlikely	Low(4)	Yes	<p>The over 350 plugins on the LMS have not been individually checked, to find out if they are collecting personal information.</p> <p>Information provided by eCreators is that the plugins do not collect information. They are there to provide functionality to the LMS only. The Blacklight results did not find any third party tracking or concerning privacy practices present on the LMS. Blacklight is a real-time website privacy inspector.</p> <p>The Executive should explore the possibility of providing online training directly through the OVIC website, and cease its engagement with eCreators and the Learnbook platform. For</p>	Very Unlikely	Minor	Low(1)	Executive Team

of confidence/trust.					<p>example, the OAIC currently provides its training directly through its website.</p> <p>Providing training directly through the OVIC website increases OVIC's control over the flow and storage of personal information, removing the increased privacy risks of using third parties, and the lack of transparency over the flows of information on an open source platform like Moodle.</p>				
----------------------	--	--	--	--	--	--	--	--	--

**Add more rows by clicking in the bottom right cell and pressing 'tab'

Use the below risk table to determine the risk rating of each identified privacy risk.

OVIC Risk Table		Select a 'Consequence Rating' from the purple row				
		Insignificant	Minor	Moderate	Major	Extreme
Select a 'Likelihood Rating' for the purple column	Almost Certain	Medium (5)	High (10)	Very High (15)	Very High (20)	Very High (25)
	Likely	Low (4)	High (8)	High (12)	Very High (16)	Very High (20)
	Possible	Low (3)	Medium (6)	Medium (9)	High (12)	Very High (15)
	Unlikely	Low (2)	Low (4)	Medium (6)	Medium (8)	High (10)
	Very Unlikely	Low (1)	Low (1)	Low (3)	Medium (4)	High (5)

Part 4 – Action items and document information

This part details any action items identified and document information. Refer to sections 18 – 22 in Part 4 of the PIA Guide (pages 33 – 38) for more information.

Action items

	<i>Action</i>	<i>Owner</i>	<i>Timeframe</i>	<i>Completed</i>
1	Document and implement a procedure to delete LMS accounts that have not been accessed for 7 or more years, user feedback on the LMS 2 years after it was provided, and Live Logs after 30 days.	Communications and Education Team	ASAP	Completed
2	Explore the possibility of providing online learning directly through the OVIC website and cease using Learnbook.	Executive, Communications and Education	ASAP	This can no longer be considered, due to reduced staffing at OVIC. R4 cannot be mitigated and must be accepted by OVIC.

**Add more rows by clicking in the bottom right cell and pressing 'tab'

Document information

<i>Title</i>	OVIC PIA – Learning Management System
<i>Location</i>	Content Manager Reference: D22/23658
<i>Owner</i>	Policy team, OVIC
<i>Consultation / Distribution</i>	Assistant Commissioner – Policy Communications team Information Security Unit Privacy and Data Protection Commissioner Privacy Officer and Chief Operating Officer Corporate Governance Committee Information Commissioner
<i>Related Documents</i>	Security and Privacy Risk Assessment Briefing Note – CM D23/1986 Elearning website security risk assessment – CM D22/22827
<i>Next review</i>	July 2024
<i>Version</i>	Version 1.0

