

Privacy Policy

Policy Particulars

Reference	BPC	Version	4
Drafted by	Manager Governance & Risk	Approved on	24 June 2026
Responsible person	Chief Operating Officer	Scheduled review date	June 2028, 2 years
Authorising Authority	Board	Endorsing Authority	Risk & Assurance Committee

Purpose

CVGT Employment (CVGT) is committed to protecting an individual’s right to privacy and considers the responsible management of personal information a key aspect of good governance.

The policy provides guidance and advice on the way in which CVGT collects, holds, uses and discloses personal information of individuals. It details how individuals can request access to their information and outlines the privacy complaint process.

Scope

This policy applies to all personal information about an individual that is collected, stored, used or disclosed by CVGT.

All employees, Board Directors, Independent Committee members, contractors and volunteers engaged by CVGT are required to adhere to this policy.

Definitions

Personal Information	Sensitive Information	Health Information
Australian Privacy Principles	Individual	

Policy

To ensure the privacy of individuals is protected, CVGT will adhere to the Australian Privacy Principles contained in Schedule 1 of the *Privacy Act 1988 (Cth)* (*Privacy Act*). CVGT’s obligations to protect personal information also includes compliance with the *Crimes Act 1914 (Cth)*.

The requirements of the *Archives Act 1983 (Cth)* relating to Commonwealth Records (including the disposal, alteration and destruction of such records) apply to CVGT’s records, including personal information.

Remaining anonymous

Individuals may use a pseudonym or remain anonymous when interacting with CVGT in most instances. However, individuals may be required to provide certain personal information for CVGT to deliver services or assess eligibility for a program or service.

CVGT will inform individuals if they are not able to remain anonymous or use a pseudonym when engaging with the organisation.

Why personal information is collected

CVGT will not request personal information that is not required. The *Privacy Act* requires that personal information is only collected for purposes that are reasonably necessary for, or directly related to, CVGT's programs or services.

CVGT may also collect sensitive information about individuals with consent, when the collection is authorised or required by law, or the collection is otherwise allowed under the *Privacy Act*.

CVGT collects, holds, uses and discloses personal information for a range of purposes related to its functions and activities, including to:

- Contact individuals to provide information about, and to deliver, services to individuals or referring organisations.
- Access and obtain medical records and history from treating healthcare providers,
- Engage healthcare providers to assist in the provision of our services and assess medical conditions and/or diagnoses,
- Provide seminars, workshops and educational training and work trial placement services,
- Promote and market the business, services and programs,
- Collate data for research and statistical purposes,
- Meet compliance requirements under the terms of deeds and contracts CVGT enters and/or administers on behalf of statutory and legislative bodies and government departments,
- Monitor, review, evaluate, develop and improve our services,
- Meet our statutory and regulatory obligations,
- Recruit personnel; and
- For other purposes required or authorised by or under law, including purposes for which you have provided your express or implied consent.

How personal information is collected

The types of personal information collected will depend on the activities and functions CVGT are undertaking. CVGT may collect personal information about individuals through surveys, email and phone communications, correspondence and submissions, forms and notices (including online portals), and via its websites. This includes:

- from the individual directly, or through their authorised representative,
- via a third party if permitted by law.

When CVGT collects personal information, individuals will be notified using a privacy collection notice, if it is reasonable to do so. The notice will include reasons why CVGT are collecting the information, whether the collection is required or authorised by law, and any person or body to whom the information is usually disclosed to.

Individuals may be asked to sign a consent form to acknowledge and provide consent to the collection of their personal information. Once completed, the consent form will be stored in an electronic database linked to the individual's secure electronic record.

CVGT will also inform individuals how they can request access to, or correction of, their personal information, and who to contact for privacy enquiries or to make a complaint. There may be some situations where CVGT are not able to notify an individual using a privacy collection notice. See *Appendix A – Collection Notices*

Unsolicited personal information

Sometimes CVGT may receive personal information that was not requested (for example, information included in an unsolicited email or document). Where this occurs, CVGT will assess whether the information could have been collected in accordance with the Australian Privacy Principles. If the information could not lawfully be collected, CVGT will destroy or deidentify the information as soon as practicable, where it is lawful and reasonable to do so. If CVGT is permitted to keep the information, it will be handled in accordance with this Privacy Policy.

How personal information is safeguarded

CVGT takes seriously its obligations to protect the personal information it holds. CVGT takes reasonable steps to protect personal information against misuse, interference and loss, and from unauthorised access, modification or disclosure. These steps include:

- classifying and storing records securely per Australian government security guidelines
- internal access to information is on a 'need to know' basis and only by trained authorised personnel
- providing access to and monitoring systems with controls and authenticated credentials
- ensuring buildings are secure
- regularly updating and auditing storage and data security systems.

CVGT's IT environment has been established to meet the international standards for Information Security (ISO/IEC27001:2022) and designed to meet the Australian Signals Directorate (ASD) Essential Eight mitigation strategies and Australian Government Information Security Manual requirements. All CVGT Servers are located in secure data centres hosted inside Australia or secured on premises server rooms with Encryption at rest for all sensitive data.

CVGT may engage third party service providers to deliver or support its operations (for example, IT hosting, communications platforms, and specialist service delivery). CVGT selects and uses service providers and systems designed to keep personal information hosted and accessed within Australia. If an offshore arrangement were ever required, it would only occur where permitted by law or specific contractual requirements. Where CVGT discloses personal information to an overseas recipient, it will take reasonable steps (before the disclosure) to ensure the recipient handles the information in a way that is consistent with the Australian Privacy Principles, as required by the Privacy Act.

Where personal information relates to Services delivered under Commonwealth funding arrangements, CVGT also complies with applicable data sovereignty and security requirements, including not transferring, transmitting, permitting access to, or storing relevant records or personal information outside Australia without the Department's prior written approval.

CVGT will appropriately destroy, erase or de-identify any personal information that is no longer required for any purpose described in this policy or under any applicable laws and do not keep personal information longer than necessary. This requirement applies except where:

- the personal information is part of a Commonwealth Record, or
- it is required by law or a court/tribunal order to retain the personal information.

Personal information contained in a Commonwealth Record is managed in accordance with the *Archives Act 1983 (Cth)*.

If personal information that is held by CVGT is lost, or subject to unauthorised access or disclosure, CVGT will respond in line with the Office of the Australian Information Commissioner's Data breach preparation and response – a guide to managing data breaches in accordance with the *Privacy Act* and the CVGT's Data Breach Response Procedure. CVGT aim to provide timely advice to affected individuals if a data breach is likely to result in "serious harm". CVGT's Privacy Officer undertakes an assessment in line with the Notifiable Data Breaches scheme and the Data Breach Response Procedure to determine if the breach is likely to result in "serious harm" to one or more individuals.

The types of information CVGT holds

In performing its functions, CVGT may collect and hold the following kinds of personal information:

- identity and contact details for individuals (e.g. name, phone, email and postal address),
- information relating to an individuals' personal circumstances and health (e.g. age, gender, and family circumstances including spouses, carers and dependents),
- information relating to an individuals' financial affairs (e.g. payment details, bank account details),
- other information relating to identity (e.g. date of birth, signatures, citizenship and visa status),
- information about employment (e.g. employment status and work history, education status, referee comments, salary), and
- government identifiers (e.g. tax file number or customer reference number).

We may also collect and hold the following kinds of sensitive information:

- racial and ethnic origin,
- sexual orientation,
- biometrics (such as photographs or documents containing photos, video recordings (CCTV) and audio recordings of individuals),
- religious, cultural and linguistic background,
- health (including information about an individual's medical history and any disabilities or injuries)
- information about political or union memberships and associations, and
- information about criminal activities individuals may have been involved in.

Biometric information may be captured on CVGT premises and when communicating with us for safety, security and operational purposes. Where CVGT discloses this information to law enforcement, CVGT will only do so when an individual has consented or where CVGT is required or authorised by law to do so.

CVGT may also collect information about how individuals use its online services and applications. For example, CVGT use social networking services such as Facebook, "X" (Twitter) and LinkedIn to talk with the public and its staff. These services have their own privacy policies. Access to the privacy policies for these services is on their websites. When individuals interact with CVGT using these platforms, personal

information may be collected for communication purposes. These social networking platforms will also handle an individual's personal information for their own purposes.

How information is used and disclosed

CVGT uses and discloses collected personal information for the primary purpose of collection. CVGT will take reasonable steps to inform individuals of the reason for collection at or as soon as practicable after the time of collection.

CVGT may also use and disclose personal information for a secondary purpose, where permitted under the Privacy Act. This may include where:

- the individual has consented to the use or disclosure; or
- the individual would reasonably expect the use or disclosure, and it is related to the primary purpose of collection (or directly related for sensitive information); or
- the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order; or
- another permitted exception applies under the Privacy Act.

CVGT may disclose an individual's personal information to:

- the organisation that referred the individual to CVGT services
- medical practitioners and / or allied health professionals engaged by CVGT to provide services
- the individual's treating healthcare providers
- persons or organisations assisting CVGT in carrying out its functions
- parties involved in a prospective or actual transfer of our assets or business
- other organisations engaged or contracted by CVGT to assist with the delivery of its functions and / or provide services.

Such organisations may include:

- recruitment agencies,
- previous employers,
- credit agencies,
- state or federal police,
- state or federal government agencies or departments, or
- conformity assessment bodies.

CVGT may also disclose sensitive information regarding memberships of trade and professional associations and general information to government agencies, lawyers and other third parties who deal with CVGT as part of its delivery of services.

CVGT may disclose personal information to overseas recipients when that disclosure is consistent with the purposes of collection.

Direct marketing

CVGT will only use or disclose personal information for direct marketing, where permitted by the Privacy Act. When CVGT send direct marketing communications, a simple way to opt out will provided (for example, an unsubscribe link or contact method) and CVGT will comply with opt-out requests. If an individual requests information about the source of their personal information used for direct marketing, CVGT will provide this information unless it is unreasonable or impracticable to do so.

Releasing protected information to a third party (including the police) using a Public Interest Certificate

The *Social Security (Administration) Act 1999 (Cth) (SS(Admin) Act)* prohibits any person from misusing information about a person that is or was held in a Commonwealth Record for social security purposes.

Protected information is defined in the *Social Security Act 1991 (Cth)* as “information about a person that was obtained by an officer under the social security law; and is held or was held in the records of the Department or the Human Services Department”.

In limited circumstances, the Secretary can determine that protected information can be disclosed if it is in the public interest. The disclosure of that protected information is released by a Public Interest Certificate (PIC).

A PIC identifies the personal information that can be released about an individual; who it can be released to; who can release the information; and allows the information to be released if it is necessary in the public interest to do so. (Refer to the Release of Information Procedure.)

Using CVGT’s Website

When using CVGT’s website, personal information provided by individuals may be collected. CVGT use network tools to identify web browsers, this may include the use of cookies and other technologies. Cookies are used to assist in enhancing an individual’s browsing experience. Cookies do not reveal an individual’s email address; however, this may be recorded when an individual transmits it to CVGT electronically in an email message or through a web e-form. CVGT’s website may contain links to other websites; this privacy policy has no application to any other website.

Accessing personal information

Individuals may request access to their personal information held by CVGT by making a request in writing addressed to the Privacy Officer at privacy@cvgt.com.au detailing:

- the individual’s name and contact details,
- the personal information being requested,
- the time period for which the request relates,
- the individual’s preferred method of receiving access to the personal information (such as receiving a copy by email or post, or just wanting to look at the information), and
- details of any person or organisation the individual authorises to access the personal information on their behalf.

CVGT must be satisfied the request is being made by the individual or an authorised person and will require a minimum of 4 unique points of identification, including:

- Full Name
- Date of Birth
- Address
- Phone / Email

CVGT may also ask for additional information to confirm an individual’s identity.

The Privacy Officer will confirm further details regarding the procedure and timeframes following a request for information. CVGT will typically respond to requests within 30 days, however there may be delays associated with the nature of the information requested.

Requesting access to personal information is generally free, however CVGT may charge a reasonable administration fee if permitted for providing you access.

The charge may include the cost of:

- staff searching for, locating and retrieving the requested information, and deciding which personal information is relevant to the request,
- staff reproducing and sending the personal information, and
- the postage or materials involved in giving access.

CVGT will advise the individual of the likely amount of the charge when making the request as well as options to minimise any charges.

When an individual requests their personal information contained within a Commonwealth Record, CVGT will not charge for providing access.

If CVGT withholds access in accordance with the *Privacy Act*, written reasons for withholding the information will be provided.

Updating and correcting personal information

It is important that personal information is accurate, complete and up to date for CVGT to perform its services.

CVGT takes reasonable steps to ensure that personal information collected is accurate, up to date and complete. CVGT will also take reasonable steps to ensure that at the time of use or disclosure of any personal information, it is accurate, up to date, complete and relevant.

CVGT may request individuals to advise of any changes to their personal information.

Individuals have a right to request the correction of their personal information by writing to the Privacy Officer.

CVGT will take all reasonable steps to correct personal information when the inaccuracy is identified by CVGT or when an individual requests CVGT to correct or update their information. If CVGT correct the information, all relevant stakeholders will be advised.

If CVGT is unable to correct an individual's personal information, a notice outlining the reasons why the correction requested has not been made and available complaint mechanisms.

If CVGT is unable to correct an individual's personal information, they may request a statement be associated with the personal information noting that the individual believes it is inaccurate, out of date, incomplete, irrelevant or misleading. CVGT will take reasonable steps to associate that statement with the relevant record.

How to make a privacy complaint

Individuals who are not satisfied with how CVGT have collected, held, used, or disclosed their personal information, can make a formal complaint to the Privacy Officer.

The complaint should include:

- A short description of the privacy concern,
- Details of any prior interactions with staff of CVGT to address your concern; and
- Preferred contact details.

CVGT will respond to a complaint within 30 days of receiving the written complaint.

If the complaint is not resolved, individuals may lodge a complaint with the Office of the Australian Information Commissioner (OAIC).

The OAIC can receive privacy complaints through:

- the online Privacy Complaint form (refer to the OAIC's website),
- by email (email that is not encrypted can be copied or tracked) at enquiries@oaic.gov.au
- by mail (if you have concerns about postal security, consider sending your complaint by registered mail) to:

Office of the Australian Information Commissioner
Sydney Offices
GPO Box 5218
Sydney NSW 2001

- by fax at +61 2 9284 9666

How to contact CVGT's Privacy Officer

Individual's may contact CVGT's Privacy Officer to:

- Ask questions about this privacy policy, or request a copy of this policy in an alternative format,
- Obtain access to or seek correction of personal information held by CVGT, or
- Make a privacy complaint about CVGT.

Email: privacy@cvgt.com.au

Post: The Privacy Officer
CVGT Employment
PO Box 473
Bendigo VIC 3552

Privacy Impact Assessments

A Privacy Impact Assessment Threshold Test (PIATT) will be completed for all new projects to determine if a Privacy Impact Assessment is required. Completed PIATT's must be provided and approved to the Privacy Officer prior to commencing the project. See *Appendix B – Privacy Impact Assessment Threshold Test*.

A PIA identifies how the new or revised project, activity or system can have an impact on an individual's privacy, and makes recommendations for managing, minimising or eliminating those privacy impacts. PIA's must be completed using the CVGT PIA Tool (Appendix C), which is used to assess the proposal, document findings, and respond to recommended actions.

Where the PIATT identifies a significant change to the collection, use or disclosure of personal information, or where advised by the Privacy Officer the Office of the Australian Information Commissioner (OAIC) PIA Tool ([Privacy impact assessment tool | OAIC](#)), must be used to conduct the assessment, document the findings and address recommendations.

All PIA's are to be completed in consultation with the Privacy Officer.

Exclusions

The *Fair Work Act 2009 (Cth)* requires employers to keep certain personal information about employees in their employee record including:

- the employee's personal and emergency contact details,
- information about terms and conditions of employment,
- wage or salary details,
- leave balances,
- records of work hours,
- records of engagement, resignation or termination of employment,
- information about training, performance and conduct,
- taxation, banking or superannuation details, and
- union, professional or trade association membership information.

Personal information held by an employer, relating to someone's current or former employment, isn't subject to the requirements of this policy. The *Privacy Act* and consequently the Australian Privacy Principles (APP) do not apply when the employee's personal information is only used by the employer directly in relation to their employment. Outside of employment purposes the APPs apply.

Definitions

Definition	Description
Personal Information	Defined in the <i>Privacy Act 1988 (Cth)</i> as information or an opinion about an identified individual, or an individual who is reasonably identifiable: <i>(a) whether the information or opinion is true or not; and</i> <i>(b) whether the information or opinion is recorded in a material form or not.</i>
Sensitive Information	Defined in the <i>Privacy Act 1988 (Cth)</i> as <i>(a) information or an opinion about an individual's:</i> <i>(i) racial or ethnic origin; or</i> <i>(ii) political opinions; or</i> <i>(iii) membership of a political association; or</i> <i>(iv) religious beliefs or affiliations; or</i> <i>(v) philosophical beliefs; or</i> <i>(vi) membership of a professional or trade association; or</i> <i>(vii) membership of a trade union; or</i>

	<p>(viii) sexual orientation or practices; or</p> <p>(ix) criminal record;</p> <p>that is also personal information; or</p> <p>(b) health information about an individual; or</p> <p>(c) genetic information about an individual that is not otherwise health information; or</p> <p>(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or</p> <p>(e) biometric templates.</p>
Health Information	<p>Defined in the <i>Privacy Act 1988 (Cth)</i> as information or an opinion about:</p> <p>(i) the health, including an illness, disability or injury, (at any time) of an individual; or</p> <p>(ii) an individual's expressed wishes about the future provision of health services to the individual; or</p> <p>(iii) a health service provided, or to be provided, to an individual;</p> <p>that is also personal information;</p>
Australian Privacy Principles	<p>A set of 13 principles set out in Schedule 1 of the <i>Privacy Act 1988 (Cth)</i> that regulate how personal information is handled.</p>
Individual	<p>Defined in the <i>Privacy Act 1988 (Cth)</i> as a natural person.</p>

Relevant Legislation

Archives Act 1983 (Cth)

Crimes Act 1914 (Cth)

Fair Work Act 2009 (Cth)

Privacy Act 1988 (Cth)

Social Security Act 1991 (Cth)

Social Security (Administration) Act 1999 (Cth)

Related Documents

- Appendix A - Collection Notices
- Appendix B - Privacy Impact Assessment Threshold Test
- Confidentiality Policy
- Data Breach Response Procedure
- Release of Information Procedure
- Security Camera Procedure

Breach of policy

A breach of this policy is grounds for disciplinary action, up to and including termination of employment.

Version History

Version	Latest review date	Revision Date	Summary of changes
1	29 July 2020	October 2021	Approved and adopted by the Board
2	28 October 2021	October 2022	Updated to new format and amendments to APP policy.
3	28 February 2024	February 2026	Substantial review to incorporate alignment with APPs, remove duplication between policy and procedure and separate out confidentiality elements.
4	24 June 2026	June 2028	Alignment to new Policy template and introduction of a Privacy Impact Assessment Threshold Test checklist and shortform Privacy Impact Assessment replacing the use of the OAIC template other than when required by the Privacy Officer.

APPENDIX A – Collection Notices

What is a collection notice?

The *Privacy Act 1988 (Cth)* and Australian Privacy Principle (APP) 5 requires CVGT to take reasonable steps to notify individuals of certain matters when collecting personal information.

It is important to include a collection notice to ensure individuals can provide informed consent for the collection, storage, use and/or disclosure of their personal information.

A collection notice should inform individuals about how their personal information will be handled, including:

- the purpose for which CVGT is collecting their personal information-
- whether CVGT will pass their information on to third parties-
- that further information can be found in CVGT's privacy policy.

What should a collection notice include?

The content of a collection notice is set out in APP 5.

The privacy notice should address each of the following points:

- who is collecting the information (must identify CVGT, and if applicable the State or Federal Government program)
- why the personal information is being collected
- what the personal information will be used for (this must include all uses of the personal information)
- who the personal information will be accessed by
- who the personal information will be disclosed to
- how the individual can opt out/withdraw consent in future
- the consequences if personal information is not collected
- a contact for further information
- a link to the CVGT Privacy Policy.

When should a collection notice be used?

Collection notices should be included whenever personal information (including sensitive information) is collected by CVGT. This includes collection via online and in person (electronic or hardcopy).

The notice must be provided to the individual before, or at the time, that the personal information is collected.

It is a requirement under the Privacy Act 1988 to include a collection notice on communications that are managed on a consent basis, with details about how recipients may opt out.

Example collection notices have been provided for common activities that collect personal information.

Example collection notices

Email/distribution list sign-up

Privacy Collection Notice: The information on this form is being collected by CVGT Employment.

The information is being collected, with your consent, to provide you with regular updates on <<distribution list name>>.

The information will be used by authorised staff for the purpose for which it was collected, and any other purpose which you have expressly consented to.

You can opt out of this mailing list at any time by unsubscribing <<opt-out instructions>>.

If you do not provide all the information that is requested on this form, it may not be possible for us to add your details to the distribution list.

CVGT is committed to protecting personal information provided by you in accordance with the *Privacy Act 1988 (Cth)* and the information will be protected against unauthorised access and use.

All information collected by CVGT is governed by the CVGT Privacy Policy ([hyperlink](#)).

For further information about how CVGT deals with personal information, please refer to CVGT's Privacy Policy or contact the CVGT Privacy Officer at privacy@cvgt.com.au

You may access or request correction of any personal information you have provided to CVGT by contacting privacy@cvgt.com.au

Email/distribution list communications-

Privacy Collection Notice: You have received this email from CVGT Employment, because you are subscribed to the <<distribution list name>>.

To unsubscribe please <<opt-out instructions>>.

CVGT is committed to protecting personal information provided by you in accordance with the *Privacy Act 1988 (Cth)* and the information will be protected against unauthorised access and use.

All information collected by CVGT is governed by the CVGT Privacy Policy ([hyperlink](#)).

For further information about how CVGT deals with personal information, please refer to CVGT's Privacy Policy or contact the CVGT Privacy Officer at privacy@cvgt.com.au

You may access or request correction of any personal information you have provided to CVGT by contacting privacy@cvgt.com.au

APPENDIX B – Privacy Impact Assessment Threshold Test (PIATT)

Overview

This form is to be used for any new, varied or renewed project, function or activity being undertaken within CVGT.

Instructions

Answer the following questions. If you require assistance, please contact the Privacy Officer.

The following terms are used in this document and have the following meanings.

- **PII** - Personal Identifiable Information (can include personal and sensitive information)
- **Collection** - includes personal information collected by any means, including hardcopy paper documents, audio, visual and other media.
- **Storage** - includes personal information created and stored on CVGT's systems, including both electronic and hardcopy documents.
- **Use** - includes any use, even those permitted by CVGT Privacy Policy or with consent.
- **Disclose** - includes disclosure internally and externally to CVGT.

	No	Yes	Description
Question 1 Will the CVGT project, function or activity result in the collection of PII?	<input type="checkbox"/> Go to Question 2	<input type="checkbox"/> Complete Description and go to Question 2	Describe what PII is being collected:
Question 2 Will the CVGT project, function or activity result in the storage of PII?	<input type="checkbox"/> Go to Question 3	<input type="checkbox"/> Complete Description and go to Question 3	Describe what PII is being stored:
Question 3 Will the CVGT project, function or activity result in the use of PII?	<input type="checkbox"/> Go to Question 4	<input type="checkbox"/> Complete Description and go to Question 4	Describe what PII is being used:
Question 4 Will the CVGT project, function or activity result in the disclosure of PII?	<input type="checkbox"/> Go to Question 5	<input type="checkbox"/> Complete Description and go to Question 5	Describe what PII is being disclosed:
Question 5 Has the collection, storage, use or disclosure been previously assessed and found compliant?	<input type="checkbox"/> A PIA is required. See Note 1	<input type="checkbox"/> A PIA is not required. See Note 2	Note 1: Contact the Privacy Officer to complete a Privacy Impact Assessment Note 2: Provide a copy of this PIA to the Privacy Officer for review and approval prior to commencing the project, function or activity.



Month 20XX

CVGT Privacy Impact Assessment

ADD PROJECT NAME HERE

AUTHOR NAME

Step 1 – Plan the PIA & Describe the Project

Area	Assessment Prompt	Response/Details
Project Overview	<p>Provide a brief description of the project or initiative, including its purpose, scope, and key activities.</p> <p>(Digital projects include a link to the Project Canvas)</p>	
Personal Information Involved	<p>Describe the types and approximate volume of personal information handled and specify whether any sensitive information is involved.</p>	
Public / Stakeholder Sensitivity	<p>Assess the likely level of community, participant, or media interest in the privacy aspects of the project and outline any factors contributing to heightened sensitivity.</p>	
Prior PIA Assessments	<p>Do any prior PIAs, privacy reviews, or risk assessment(s) exist that can be leveraged or updated to address privacy risks associated with the current proposal? Yes/No</p> <p>If Yes, contact the Privacy Officer prior to commencing the project, function or activity to determine whether the prior assessment(s) can be relied on or require update.</p>	

Step 2 – Stakeholders & Consultation

Consultation may be planned or completed. As consultation progresses, any changes to the project or new privacy issues identified through consultation must be reflected in an updated or revised PIA.

List stakeholders who are, or might be, impacted by the project.	Describe the impact of the project on each stakeholder, particularly in relation to the collection, use, disclosure, or handling of personal or sensitive information.	Describe the consultation approach (e.g. meetings, workshops, surveys, communications).	Summarise key issues, concerns, or feedback raised by stakeholders during consultation.	Describe how stakeholder feedback informed or influenced project design, controls, mitigations, or decision-making.

Step 3–Map Information Flow

Describe the information flow using the table below or insert or reference an information flow diagram.

Information collected	Source of Collection	Use and Disclosure	Storage and Location	Access Controls	Retention and Disposal
What personal and/or sensitive information is collected or generated as part of this activity?	From whom or where is the information collected (e.g. individual, employee, third party, system-generated)?	How is the information used, and is it disclosed or shared with any internal or external parties? If yes, identify who and for what purpose.	Where is the information stored (e.g. system, platform, physical location)?	Who has access to the information? What rights do they have? (e.g. read only, read/write, edit and admin)	How long is the information retained?

Step 4–Privacy Impact Analysis & Compliance Check

CVGT maintains a clear, current and easily accessible Privacy Policy that meets the requirements of the Australian Privacy Principles (APPs). The policy outlines how privacy enquiries and complaints are managed.

Key Considerations for this project include:

Privacy Area	Assessment Prompt	Response (Yes / No / N/A)	Details / Evidence / Actions
Alignment with the Privacy Policy	Is the collection, storage, use, access or disclosure of personal information consistent with CVGT's Privacy Policy? If No, can the activity proceed as proposed, or does the Privacy Policy require amendment before progressing?		<i>If No identify required policy changes, risks, approval pathway, and interim controls.</i>
Collection Notices	Will personal information be collected or used as part of this activity?		<i>Specify types of information and point of collection.</i>
	Will a collection notice be provided to individuals at or before the time of collection?		<i>Attach or reference the notice and delivery method (e.g. form, portal, website).</i>
	If No, why is a collection notice not being provided and how will individuals otherwise be informed?		<i>Explain justification, transparency measures, and privacy risk implications.</i>

Direct Marketing	Will personal information be used or disclosed for direct marketing purposes?		<i>If yes, describe consent, opt-out mechanisms, and compliance controls.</i>
-----------------------------	---	--	---

Step 5 – Privacy Management – Addressing Risks

Through the privacy impact analysis, you may have identified risks to privacy in the project’s current design. Document and assess each of the risk in the table below. Refer to CVGT’s risk management framework (policy & procedure) for guidance on how to describe the risk and determine the likelihood and consequence ratings.

Privacy Risk Description	Risk Mitigation / Treatment Actions	Residual Likelihood	Residual Consequence	Residual Risk Rating	Risk Owner
Describe the privacy risk, focusing on potential impact to individuals (e.g. unauthorised access, over-collection, lack of transparency, misuse or disclosure).	Describe existing controls and any additional mitigation actions required (policy, technical, procedural), including timeframes if applicable.				

Step 6 – Summary of Recommendations

Detail a list of actionable recommendations to remove/minimise/mitigate risks

Recommendation Clearly describe the action required (policy, process, system, communication, training, control).	Privacy Risk Addressed Reference the relevant privacy risk(s) mitigated	Residual Risk Remains? (Yes/No)	If Yes – Residual Risk Description & Impact Describe the remaining risk to individuals and any operational, reputational, or compliance impact to CVGT.	Acceptable Risk? (Yes / No)	Justification for Acceptance of Risk? Clearly describe the reasons why the risk is acceptable	Owner

Step 7 – Response to Recommendations – Action Plan

Prepare an action plan for implementing the recommendations, indicating a specific timeframe for remedying or mitigating the risks that have been identified and who is responsible for the implementation.

Action Clearly describe the action to be taken (e.g. update collection notice, amend policy, implement system control, provide training).	Related Recommendation / Risk Reference the relevant PIA recommendation or privacy risk being addressed.	Action Owner	Timeframe Specify due date or milestone.	Completion Status / Date Completed Record status (e.g. Not started / In progress / Completed) and date completed.

Step 8–Update PIA if required

Many projects undergo changes before they are finally implemented. As the project progresses, the PIA should be revisited and updated or revised if developments in the design or implementation of the project create new privacy impacts that were not previously considered. If the changes are substantial and result in significant new privacy impacts that were not considered in the PIA, it may be necessary to undertake a new PIA.