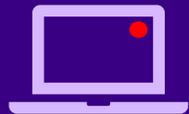


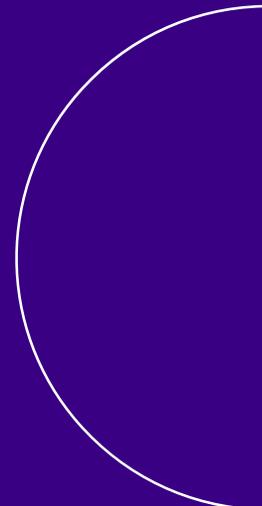
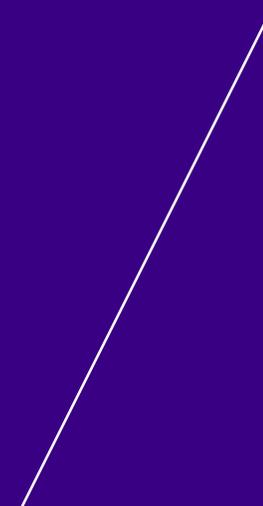
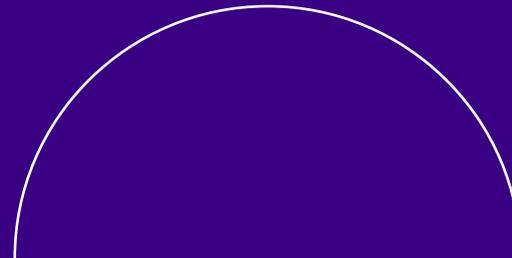


# Class B Cemetery Trusts and Committees of Management Preparing for the 2026 Protective Data Security Plan

Information Session  
February 2026



A reminder – Today's session  
is being recorded.



# Acknowledgment of Country

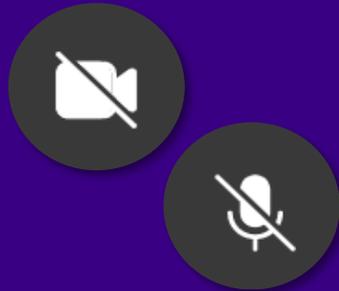
**Laurencia Dimelow**

Acting Assistant Commissioner

We acknowledge the Wurundjeri people of the Kulin Nation as the Traditional Owners of the land from which we are presenting today.

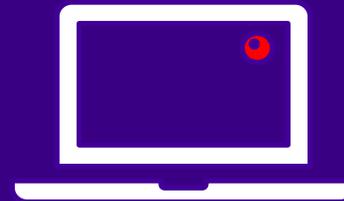
We pay our respects to their Elders, past and present, and Aboriginal Elders of other communities who may be with us today.

# Housekeeping - What to be aware of

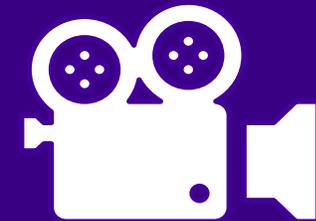


During the presentation **cameras and mics** have been **muted** for attendees.

At the end of the presentation, you will have to opportunity to come off mute to ask questions.

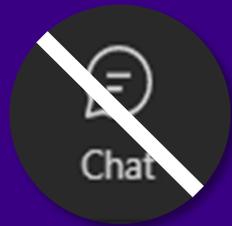


Today's session is **being recorded**.



A copy of OVIC's **slides** and the **recording** will be made available in the coming days on our website.

# Housekeeping – How to engage



Regular **chat functionality** in Teams has been **disabled** in this forum.



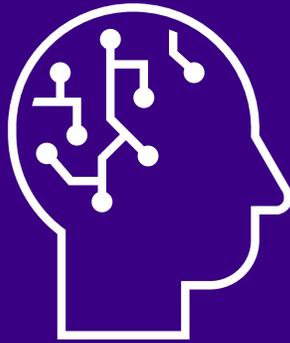
If you want to ask questions, please use the **Teams Q&A channel**.

There is an option to remain **anonymous**.



Each speaker will answer questions following the presentation. If you prefer to ask your question verbally, **raise your hand and come off mute when called upon**.

# Housekeeping – Use of AI tools



Slides and a recording of this session will be made available in the coming days.

As such, we ask that no Generative AI tools are used to take notes or record this event. We will remove users/tools if there is suspected Gen AI use.

## OVIC's position on the use of generative AI in meetings with OVIC

A PDF document of this information is available to view and download [here](#).

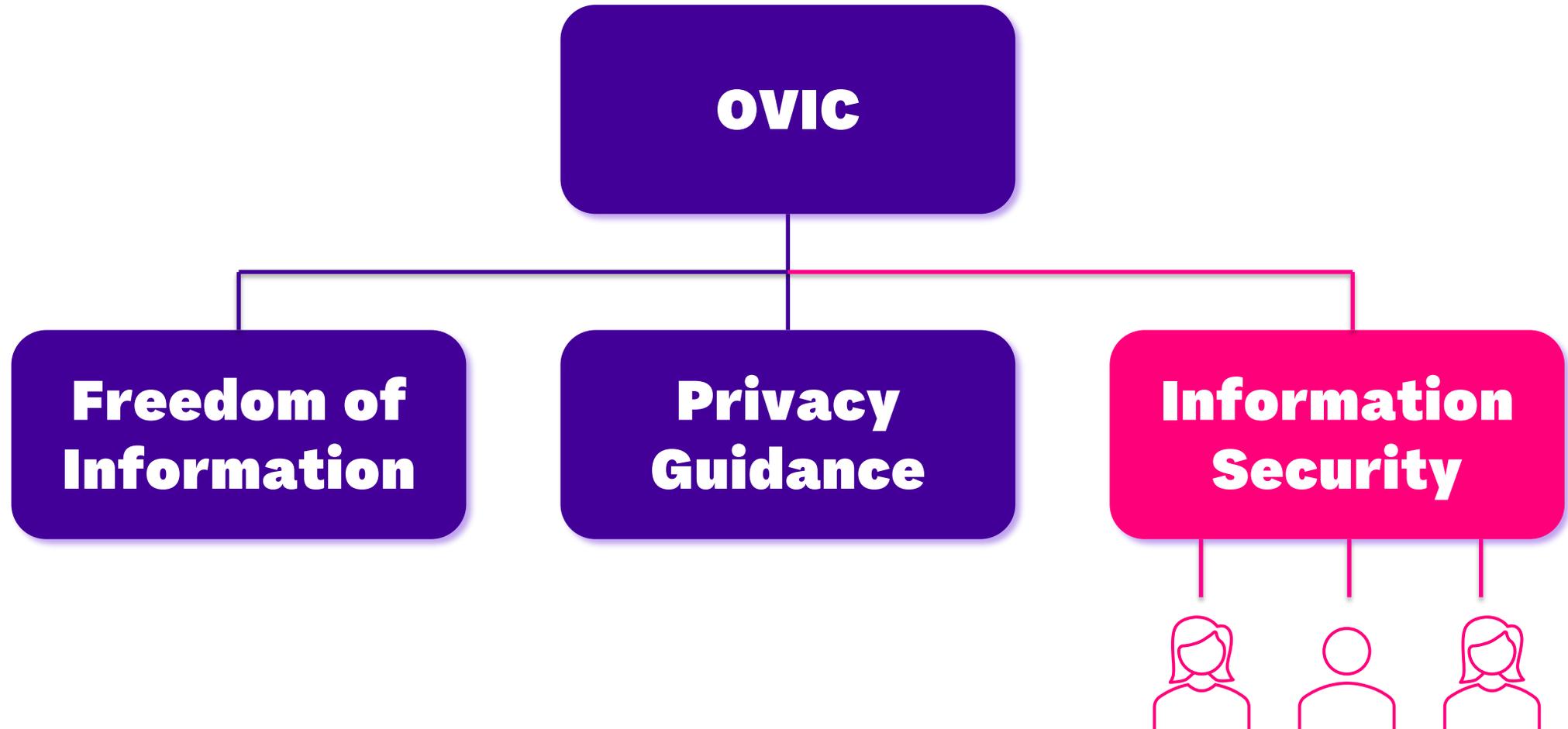
This article outlines the Office of the Victorian Information Commissioner's (**OVIC**) position on the use of generative AI tools including AI notetakers, in meetings between OVIC's staff and OVIC's stakeholders.

OVIC's stakeholders may include Victorian public sector organisations, local councils, contracted service providers, consultants, Members of Parliament, interstate and international colleagues, and members of the public.

OVIC's staff includes OVIC employees and statutory office holders.

<https://go.vic.gov.au/4fM3O3t>

## Who we are



## Today's agenda

## Purpose of today's session

Today's session is targeted to both:

- Class B Cemetery Trust members
- Committee of Management members

Some attendees today will be somewhat familiar with these requirements and will be using this session as a refresher.

For those who are not, we encourage you to take advantage of this session to understand the purpose of the Protective Data Security Plan (**PDSP**) and how it can help protect the information your trust or committee.

## What we'll explore today



Why is a Protective Data Security Plan (**PDSP**) needed?



Simplified reporting for Class B CTs & CoMs



Breaking down the PDSP



An example: reading and responding to the requirements



Submission process



Questions



Final thoughts and getting more information



# Why is the Protective Data Security Plan needed?

Class B Cemetery Trusts

Committees of Management of Crown land reserves



# Background:

## The legislation

Privacy and Data Protection Act 2014  
No. 60 of 2014  
Part 4—Protective data security

### Part 4—Protective data security

#### Division 1—Application of Part

##### 84 Application of Part

- (1) Subject to subsection (2), this Part applies to—
  - (a) a public sector agency; and
  - (b) a body that is a special body, within the meaning of section 6 of the **Public Administration Act 2004**; and
  - (c) a body declared under subsection (3) to be a body to which this Part applies.
- (2) This Part does not apply to the following—
  - (a) a Council;
  - (b) a university within the meaning of the **Education and Training Reform Act 2006**;
  - (c) a body to which, or to the governing body of which, the government of another jurisdiction, or a person appointed or body established under the law of another jurisdiction, has the right to appoint a member, irrespective of how that right arises;
  - (d) a public hospital within the meaning of the **Health Services Act 1988**;
  - (e) a public health service within the meaning of the **Health Services Act 1988**;
  - (f) a multi-purpose service within the meaning of the **Health Services Act 1988**;
  - (g) an ambulance service, within the meaning of the **Ambulance Services Act 1986**.
- (3) The Governor in Council, by Order published in the Government Gazette, may declare a body to be a body to which this Part applies.

Authorised by the Chief Parliamentary Counsel  
109

In 2014, the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) was passed by the Victorian Parliament, ushering in Australia's first broad-based legislated information security requirements.

The PDP Act empowers the Victorian Information Commissioner to:

- develop the Victorian Protective Data Security Framework for monitoring and assuring public sector data security, and
- issue the Victorian Protective Data Security Standards (**the 'Standards'**).



# Who the legislation applies to:

## Class B cemetery trusts and Committees of management

The PDP Act applies to a vast range of agencies and bodies, including:

- Class B Cemetery Trusts (**Class B CTs**) under the *Cemeteries and Crematoria Act 2003* (Vic) are considered to be public entities for the purposes of the *Public Administration Act 2004* (Vic)

and

- Committees of management of Crown land reserves (**CoMs or 'Committees of Management'**) under the *Crown Land (Reserves) Management Act 1978* (Vic) are considered to be public entities for the purposes of the *Public Administration Act 2004* (Vic)

**Public entities are subject to Part 4 of the *Privacy and Data Protection Act 2014* (Vic)**



**Victorian Public Service agencies / organisations**



**Class B cemetery trusts**



**Committees of management of Crown land reserves**



# Community benefits:

## Protecting community information and history

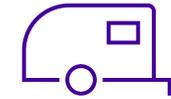
From our discussions with Class B CTs and Committees of management, it is clear that volunteers are passionate about protecting information including hard copy and soft copy (digital / electronic) information, and verbal discussions.



### Class B cemetery trusts

Documenting processes and safeguarding records benefits your community by:

- Commemorating the lives of community members
- Contributing to important genealogical records
- Strengthening the longevity of your cemetery trust for future generations.



### Committees of management of Crown land reserves

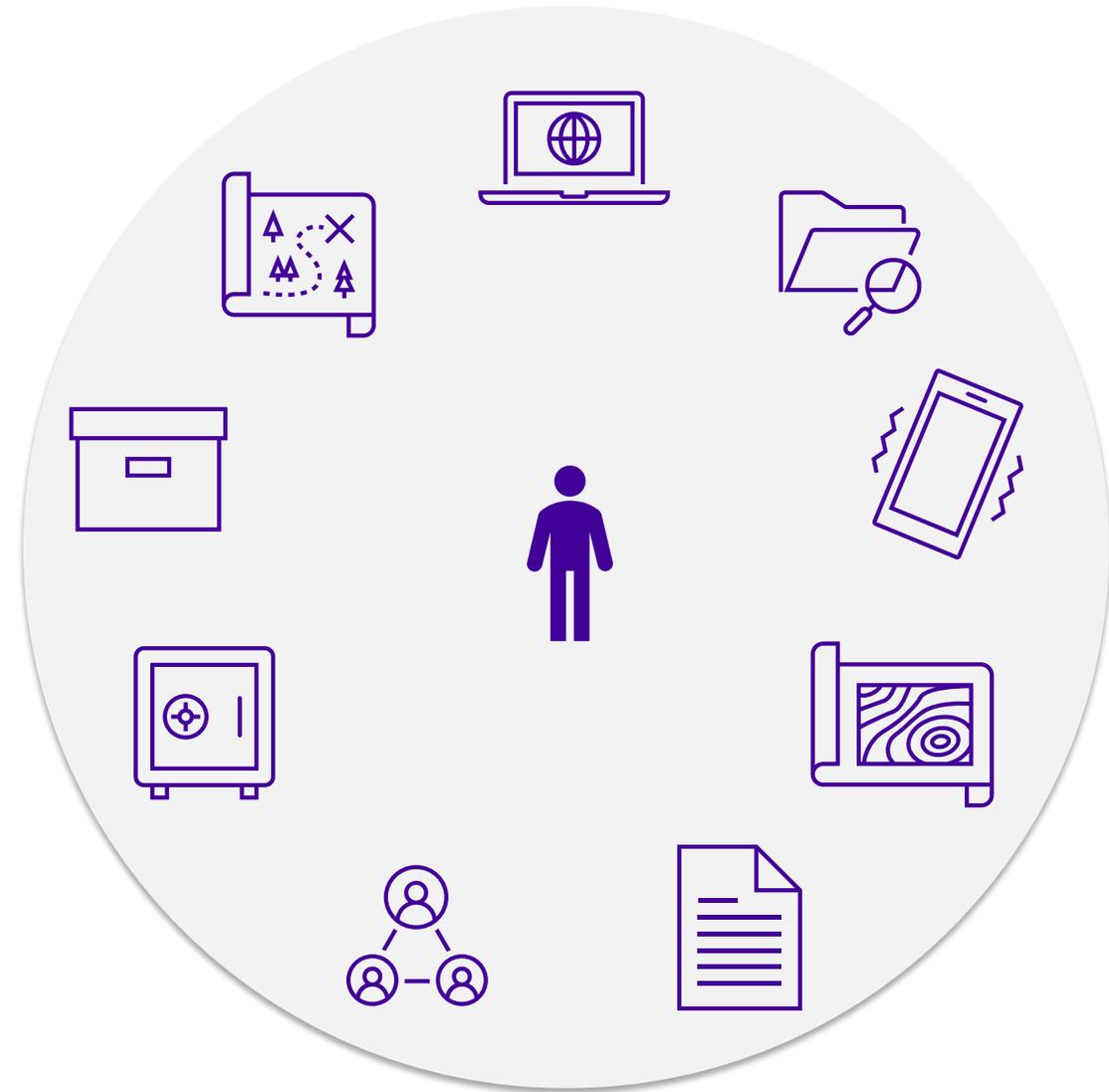
Documenting processes and safeguarding records benefits your community by:

- Commemorating historical structures and their importance
- Contributing to the maintenance and upkeep of communal places
- Providing overview of the broad amount of work that volunteers conduct.



## What: is information security?

Information security is about ensuring the **right people** have access to the **right information** at the **right time**.





# What: the legislation requires

## Information security

Under Part 4 of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**), Class B Cemetery Trusts are responsible for protecting the information they generate, hold and manage, ensuring the right people have access to the right information at the right time. This includes securing systems that hold or transmit this information.

### Legislative information security obligations

Under Part 4 of the PDP Act<sup>3</sup> a Class B Cemetery Trust (**Class B CT**) must ensure that:

- it does not do an act or engage in a practice that contravenes a [Victorian] protective data security standard (**VPDSS** or **Standard**), in respect of public sector data [Class B CT information] collected, held, managed, used, disclosed or transferred by it and public sector data systems [Class B CT systems] kept by it.
- a contracted service provider [third party] of the agency or body [the Class B CT] does not do an act or engage in a practice that contravenes a protective data security standard in respect of public sector data collected, held, used, managed, disclosed or transferred by the contracted service provider for the agency or body.
- a security risk profile assessment is undertaken for it, including an assessment of any contracted service provider of the agency or body to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body.
- a protective data security plan (**PDSP**) is:
  - developed that addresses the Standards applicable to that agency or body.
  - developed that also addresses compliance by any contracted service provider of the agency or body with the protective data security standards, to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body.
  - reviewed if there is a significant change in the operating environment or the security risks relevant to the agency or body.
- a copy of the PDSP is given to the Information Commissioner.

### Addressing the Standards as a Class B Cemetery Trust

As outlined, a Class B CT is required to develop and submit a copy of its completed PDSP. A PDSP outlines the minimum information security measures a trust will implement to ensure its information and systems are managed in a risk-informed way. OVIC has developed a PDSP template and 'How-to' guide specifically for Class B CTs.

### Mapping the Standards to the Class B Cemetery Trust requirements

This PDSP form contains 14 tailored 'requirements' Class B CTs that map back to the VPDSS. By submitting this PDSP addressing the 14 requirements, the obligation under section 89 of the PDP Act to develop, review and submit a PDSP that addresses the Standards will be fulfilled. For further information, please read OVIC's 2026 *How-to Guide: Protective Data Security Plan for Class B Cemetery Trusts*.

### Incidents impacting Class B Cemetery Trust information and systems

OVIC encourages Class B CTs to contact our office if they are impacted by an information security incident that adversely affects Class B CT information or systems.

## This session today focuses on the obligation to submit a PDSP to OVIC.

To help your Class B CT or CoM understand the information security obligations set out by Part 4 of the PDP Act, we have included a page within the Protective Data Security Plan (**PDSP**) to alert you to these.

<sup>3</sup> For the full list of requirements, see section 88 and 89 of the PDP Act.



## What:

### information needs to be considered when completing the PDSP

When completing the PDSP, consider how you can protect information in all its formats:

Paper



Electronic



Verbal



**Class B cemetery trusts** handle various types of important information such as:

- applications for right of interment
- applications for interment authorisation
- applications for approval to inter cremated human remains
- applications to establish or alter a memorial or place of interment
- death certificates and other related reports
- trust records, such as correspondence, meeting minutes, financial statements, policies and procedures.



**Committees of management** handle various types of important information such as:

- committee meeting minutes/notes
- committee records, such as correspondence, financial statements
- copies of annual returns
- policies and procedures
- records of maintenance/repairs
- registers of volunteers



## Who:

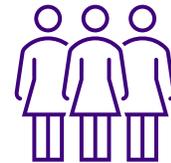
should be involved in the development and submission of a PDSP?

### Who can help complete the PDSP?



The PDSP can be completed by anyone with an understanding of the committee / trust's operations.

- Chairperson
- Treasurer
- Secretary
- Committee members
- Third parties



### Who can sign the PDSP?



The PDSP can be signed by:



The Chairperson

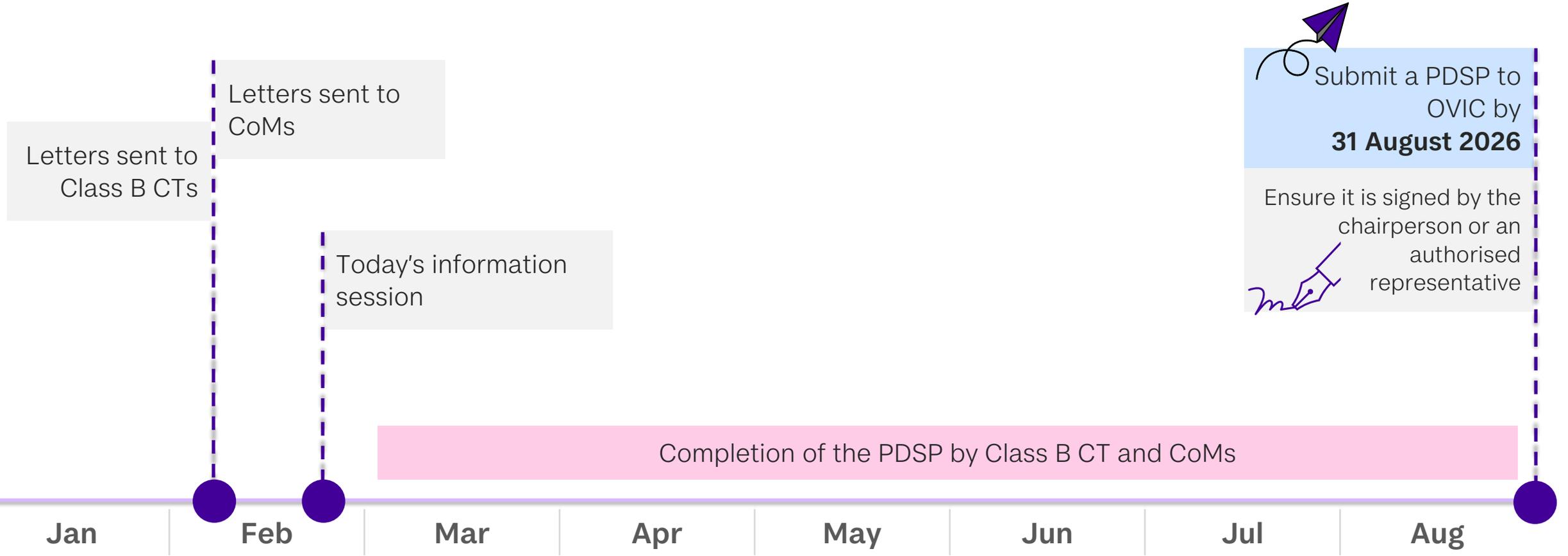
or



A representative authorised by the Chairperson



# When: is the PDSP due?



Submissions received by OVIC after 31 August 2026 will be considered late.



## How OVIC has simplified the reporting for Class B CTs and CoMs



# The Standards

Under the PDP Act, Victoria's Information Commissioner is empowered to issue Victorian Protective Data Security Standards (the 'Standards')



# 12

high level mandatory Standards made up of

# 98

elements that VPS organisations need to risk assess and implement where applicable



# 14

core requirements mapping back to the Standards

Class B CTs and CoMs must also comply with the 12 Standards.

To assist and enable this, OVIC has mapped the 12 Standards and 98 elements into **14 core Requirements.**

These 14 requirements will assist Class B CTs and CoMs in managing information in a consistent and secure manner while meeting the legislative obligations.



# The Victorian Public Sector PDSP form:

**Not** for use by Class B CTs or CoMs (reference only)

OFFICIAL

## Protective Data Security Plan (PDSP)

Single organisation PDSP form  
Version 3.7

### Information Security

Victorian Protective Data Security Standards (VPDSS)  
Reporting information security capability and implementation progress

This form is intended to be completed electronically. Different software may preview form fields differently.

The 2026 PDSP form was developed using Acrobat 2020 (0.005.30774). For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

OFFICIAL

OFFICIAL

## Standard 1 - Information Security Management Framework

An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.

### Standard 1 element assessment

Standard 1 elements	Entry Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
E1.010 The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.				
E1.020 The organisation's information security management framework contains and references all legislative and regulatory drivers.				
E1.030 The organisation's information security management framework aligns with its risk management framework.				
E1.040 Executive management defines information security functions, roles, responsibilities, competencies and authorities.				
E1.050 Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.				
E1.060 Executive management owns, endorses and sponsors the organisation's ongoing information security program(s) including the implementation plan.				
E1.070 The organisation identifies information security performance indicators and monitors information security obligations against these.				
E1.080 Executive management commits to providing sufficient resources to support the organisation's ongoing information security program(s).				
E1.090 The organisation sufficiently communicates its information security management framework and ensures it is accessible.				

Freedom of Information | Privacy | Data Protection

OFFICIAL

OFFICIAL

## Part B - Organisation summary

Organisation information and contact details

Public sector agency or body

Name of the public sector agency or body:

Preferred abbreviation of agency or body name (optional):

Organisation contacts

Public sector body Head (e.g., Department Secretary, CEO)	Information Security Lead (The organisation's nominated contact regarding the VPDSS)
Full name: <input type="text"/>	<input type="text"/>
Position title: <input type="text"/>	<input type="text"/>
Phone number: <input type="text"/>	<input type="text"/>
Email address: <input type="text"/>	<input type="text"/>
Postal address: <input type="text"/>	<input type="text"/>

In which part of the organisation does the ongoing management of the information security program reside?

Notify if 'Other' was selected:

Name of the Victorian government portfolio in which the agency or body operates under:

Notify if 'Other' was selected:

If the 'Local Government' portfolio has been selected, outline what information and system assets are covered by the PDSP.

(Multiple can be selected)

- Local Government Authority (Council) information and systems
- Committee of Management information and systems
- Class B Cemetery Trust information and systems

Freedom of Information | Privacy | Data Protection

OFFICIAL

OFFICIAL

## Part C - Attestation

This Protective Data Security Plan (PDSP) is submitted to the Victorian Information Commissioner in accordance with section 89 of the Privacy and Data Protection Act 2014 (Vic) (PDP Act).

I,  (full name) as the public sector body Head of  (organisation/agency/body) confirm that:

- my organisation has implemented the 12 Victorian Protective Data Security Standards (Standards); or is in the process of planning and/or implementing these Standards (where applicable)
- the contents of this PDSP accurately reflect the current information security risks and program of my organisation, and
- I am aware of, and acknowledge, my obligations as public sector body Head as outlined under Part 4 of the PDP Act.

Print full name:

Position title:

Date:

Insert signature or sign here:

Freedom of Information | Privacy | Data Protection

OFFICIAL

Victorian Public Sector agencies must complete this form.



27 pages addressing:

- the 12 Standards
- 98 accompanying elements
- maturity assessments



6 pages asking VPS agencies to summarise their organisation and security program.



Attestation that must be signed by the public sector body Head.



# The tailored PDSP forms: For use by Class B CTs or CoMs

OFFICIAL

**OVIC**  
Office of the Victorian Information Commissioner

2026 | Committees of management of Crown land reserves  
Protective Data Security Plan  
Version 1.0

Committee of management name: \_\_\_\_\_

**Before you start**

- Please refer to the Committee of management Protective Data Security Plan (PDSP) How-to Guide for help filling out this form.
- A completed copy of this Plan is due to the Office of the Victorian Information Commissioner (OVIC) by 31 August 2026.
- Please ensure you maintain a completed copy of this plan for your own records.
- This document has been marked as OFFICIAL by OVIC. If you feel your Committee's PDSP requires a different marking, please contact us.
- Should you require assistance in completing this form, please call 1300 006 842 or email security@ovic.vic.gov.au

OVIC Office of the Victorian Information Commissioner CoM of Crown Land Reserves 2026 Protective Data Security Plan | V1.0 Page 1

OFFICIAL

PART A – Contact information (mandatory)

	Chairperson	Person authorised by the Chairperson to submit a copy of this PDSP	Nominated point of contact (if different from the Chairperson)
Full name			
Position title	Chairperson		
Phone number			
Email address			
Postal address			

OVIC Office of the Victorian Information Commissioner CoM of Crown Land Reserves 2026 Protective Data Security Plan | V1.0 Page 5

OFFICIAL

PART B – Self-assessment against the requirements (mandatory)

Requirement 1  
The committee of management records how it securely manages its information.

The requirement maps to Standard 2 of the VPDSP: An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.

Explanation of requirement: Documentation informs all committee members (current and future) on the expectations around securely managing committee information.

Recommended supporting activity: Committee members discuss and write down their approach to securely managing committee of management of Crown land reserve (CoM) information. This should be recorded in the form of a single statement, or for more complex CoMs, it may be recorded in one or more documents.

Action required – complete the below

Current Response (tick one box)	If you select not applicable, you must provide a rationale for the selection here:	Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →		<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

OVIC Office of the Victorian Information Commissioner CoM of Crown Land Reserves 2026 Protective Data Security Plan | V1.0 Page 6

OFFICIAL

PART C – Attestation (mandatory)

The attestation must be signed by the Chairperson of the committee of management of Crown land reserves (CoM) or their authorised representative (as specified in Part A of this form).  
This Protective Data Security Plan is submitted to the Victorian Information Commissioner in accordance with section 89 of the Privacy and Data Protection Act 2014 (Vic).

I, \_\_\_\_\_ (Full Name) attest that \_\_\_\_\_ (Name of the CoM)

- has implemented the 14 requirements, or is in the process of planning and/or implementing these requirements (where applicable), as required by the Victorian Protective Data Security Standards,
- the contents of this PDSP accurately reflect the current information security risks and program of the CoM, and
- I am aware of, and acknowledge, my trust's obligations under Part 4 of the PDP Act.

I am authorised to make this attestation.

Signature \_\_\_\_\_  
Print name \_\_\_\_\_  
Position \_\_\_\_\_  
Date \_\_\_\_\_

Check this box if more than one CoM is captured by this PDSP.  
(If more you list the details of the additional CoM in Part D of this form)

OVIC Office of the Victorian Information Commissioner CoM of Crown Land Reserves 2026 Protective Data Security Plan | V1.0 Page 21

Class B CTs and CoMs must complete the form that corresponds to them. =

Part A: a page outlining the best contacts for your trust or committee. +

Part B: the 14 Requirements and optional free text field +

Part C: Attestation signed by the chairperson or an authorised representative.

CoMs or CTs that are submitting on behalf of other multiple CoMs/CTs must also fill out Part D.



## What you'll need: a Class B CT or CoM PDSP form

**2026 Class B Cemetery Trust PDSP** form (v1.3) has been released and is now available for download

<https://go.vic.gov.au/4aPHBk2>

OFFICIAL



**OVIC**  
Office of the Victorian  
Information Commissioner

2026 | Class B Cemetery Trust  
Protective Data Security Plan  
Version 1.3

Cemetery Trust name: \_\_\_\_\_

**Before you start**

- Please refer to the 2026 How-to Guide: Protective Data Security Plan (PDSP) for Class B Cemetery Trusts for help filling out this form.
- A completed copy of this Plan is due to the Office of the Victorian Information Commissioner (OVIC) by 31 August 2026.
  - Please ensure you maintain a completed copy of this form for your own records.
- This document has been marked as **OFFICIAL** by OVIC. If you feel your Cemetery Trust's PDSP requires a different marking, please contact us.
- Should you require assistance in completing this form, please call 1300 006 842 or email [security@ovic.vic.gov.au](mailto:security@ovic.vic.gov.au)



Office of the Victorian  
Information Commissioner

Class B Cemetery Trust 2026 Protective Data Security Plan | V1.3  
Page 1

OFFICIAL

**2026 Committees of management of Crown land reserves PDSP** form (v1.0) has been released and is available for download

<https://go.vic.gov.au/4qAaPZ3>

OFFICIAL



**OVIC**  
Office of the Victorian  
Information Commissioner

2026 | Committees of management of  
Crown land reserves  
Protective Data Security Plan  
Version 1.0

Committee of management name: \_\_\_\_\_

**Before you start**

- Please refer to the Committee of management Protective Data Security Plan (PDSP) How-to Guide for help filling out this form.
- A completed copy of this Plan is due to the Office of the Victorian Information Commissioner (OVIC) by 31 August 2026.
  - Please ensure you maintain a completed copy of this plan for your own records.
- This document has been marked as **OFFICIAL** by OVIC. If you feel your Committee's PDSP requires a different marking, please contact us.
- Should you require assistance in completing this form, please call 1300 006 842 or email [security@ovic.vic.gov.au](mailto:security@ovic.vic.gov.au)



Office of the Victorian  
Information Commissioner

CoM of Crown Land Reserves 2026 Protective Data Security Plan | V1.0  
Page 1

OFFICIAL



# What you'll need: the How-To Guide

OVIC has developed unique **How-to Guides** that accompany the Class B CT PDSP and the CoM PDSP. These guides will step you through the fields, provide an explanation of terms, and submission instructions.

2026 | Class B Cemetery Trust Protective Data Security Plan (PDSP) - DOCX  
Size 215.92 KB  
[Download](#)

2026 | Class B Cemetery Trust Protective Data Security Plan (PDSP) - PDF  
Size 428.32 KB  
[Download](#)

2026-How-to-Guide-Protective-Data-Security-Plan-PDSP-for-Class-B-Cemetery-Trusts.docx  
Size 890.22 KB  
[Download](#)

2026-How-to-Guide-Protective-Data-Security-Plan-for-Class-B-Cemetery-Trusts-1.pdf  
Size 485.58 KB  
[Download](#)

## Class B Cemetery Trust stakeholders

In Victoria there are often in a voluntary deliver services with

It is OVIC's position considered to and therefore g Act).

**OVIC**  
Office of the Victorian Information Commissioner

2026 | How-to Guide: Protective Data Security Plan (PDSP) for Class B Cemetery Trusts

Version 1.2

If you need help in completing the Protective Data Security Plan, call 1300 006 842 or email security@ovic.vic.gov.au

**OFFICIAL**

2026 | How-to Guide: PDSP for Class B Cemetery Trusts  
Page 1

<https://go.vic.gov.au/4rWZUcY>

Crown-land-reserves-Protective-Data-Security-Plan-V1.o.docx  
Size 215.77 KB  
[Download](#)

2026-Committee-of-Management-of-Crown-land-reserves-Protective-Data-Security-Plan-V1.o.pdf  
Size 424.26 KB  
[Download](#)

2026-How-to-Guide-Protective-Data-Security-Plan-PDSP-for-Committees-of-management-of-Crown-land-reserves.docx  
Size 873.99 KB  
[Download](#)

2026-How-to-Guide-Protective-Data-Security-Plan-for-Committees-of-management-of-Crown-land-reserves.pdf  
Size 596.44 KB  
[Download](#)

## Committees of Management of Crown Land Reserves stakeholders

In Victoria there are by approximately 1,1: under the *Crown Land*

**CoMs regulate**

It is OVIC's position purposes of the the *Privacy and regulated und*

**OVIC**  
Office of the Victorian Information Commissioner

2026 | How-to Guide: Protective Data Security Plan (PDSP) for Committees of Management of Crown land reserves

Version 1.0

If you need help in completing the Protective Data Security Plan, call 1300 006 842 or email security@ovic.vic.gov.au

**OFFICIAL**

2026 | How-to Guide: PDSP for CoM of crown land reserves  
Page 1

<https://go.vic.gov.au/3ZEhHto>



Let's do a PDSP together



## Part A – Contact information

Record the **contact information** for your Committee or Trust's:

1. Chairperson
2. Authorised representative
3. Point of contact for OVIC

OVIC understands that for some Class B CTs and CoMs, the person who is best placed to receive communications from OVIC could be the secretary, treasurer or volunteer member.

### PART A – Contact information (mandatory)

	Chairperson	Person authorised by the Chairperson to submit a copy of this PDSP	Nominated point of contact (if different from the Chairperson)
Full name	John Smith	John Smith	Jane Citizen
Position title	Chairperson	Chairperson	Secretary
Phone number	0411 222 333		9111 9222
Email address	johnsmith@cmail.com		cemetery@cemeterytrust.com.au
Postal address	123 Cemetery Lane 3XXX		PO Box 1 Melbourne 3000



# Part B – Self-assessment against Requirements

In this part of the PDSP you will find **one Requirement per page.**

Each Requirement contains 4 parts to read.

This example is showing a Class B CT PDSP, however this structure is the same for the Committee of Management PDSP.

## PART B – Self-assessment against the requirements (mandatory)

### Requirement 1

The cemetery trust records how it securely manages its information.

*This requirement maps to Standard 1 of the VPSSS*

*An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.*

#### Explanation of requirement

Documentation informs all Class B Cemetery Trust (**Class B CT**) members (current and future) on the expectations around securely managing Class B CT information.

#### Recommended supporting activity

Trust members discuss and write down their approach to securely managing Class B CT information.

This could be recorded in the form of a simple statement, or for more complex Trusts, it may be recorded in one or more documents.

#### Action required – complete the below

Current response (tick one box)	Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:
<input type="checkbox"/> Not commenced (select a proposed completion date)	
<input type="checkbox"/> Planned (select a proposed completion date)	
<input type="checkbox"/> Partial (select a proposed completion date)	
<input type="checkbox"/> Implemented	
	<input type="checkbox"/> 2026 / 2027 <input type="checkbox"/> 2027 / 2028 <input type="checkbox"/> 2028 / 2029 <input type="checkbox"/> 2029 / 2030 <input type="checkbox"/> 2030+



# Part B – Self-assessment against Requirements

## PART B – Self-assessment against the requirements (mandatory)

### Requirement 1

The cemetery trust records how it securely manages its information.

*This requirement maps to Standard 1 of the VPSSS*

*An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.*

#### Explanation of requirement

Documentation informs all Class B Cemetery Trust (Class B CT) members (current and future) on the expectations around securely managing Class B CT information.

#### Recommended supporting activity

Trust members discuss and write down their approach to securely managing Class B CT information.

This could be recorded in the form of a simple statement, or for more complex Trusts, it may be recorded in one or more documents.

#### Action required – complete the below

Current response (tick one box)	Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:
<input type="checkbox"/> Not commenced (select a proposed completion date)	
<input type="checkbox"/> Planned (select a proposed completion date)	
<input type="checkbox"/> Partial (select a proposed completion date)	
<input type="checkbox"/> Implemented	
	<input type="checkbox"/> 2026 / 2027 <input type="checkbox"/> 2027 / 2028 <input type="checkbox"/> 2028 / 2029 <input type="checkbox"/> 2029 / 2030 <input type="checkbox"/> 2030+

**The Requirement** is set out at the top of the page and should be read first.



# Part B – Self-assessment against Requirements

## PART B – Self-assessment against the requirements (mandatory)

### Requirement 1

The cemetery trust records how it securely manages its information.

*This requirement maps to Standard 1 of the VPDSS*

*An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.*

Documentation informs all Class B Cemetery Trust (Class B CT) members (current and future) on the expectations around securely managing Class B CT information.

Trust members discuss and write down their approach to securely managing Class B CT information.  
  
This could be recorded in the form of a simple statement, or for more complex Trusts, it may be recorded in one or more documents.

#### Action required – complete the below

Current response (tick one box)	Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here: <input type="checkbox"/> 2026 / 2027 <input type="checkbox"/> 2027 / 2028 <input type="checkbox"/> 2028 / 2029 <input type="checkbox"/> 2029 / 2030 <input type="checkbox"/> 2030+
<input type="checkbox"/> Not commenced (select a proposed completion date)	
<input type="checkbox"/> Planned (select a proposed completion date)	
<input type="checkbox"/> Partial (select a proposed completion date)	
<input type="checkbox"/> Implemented	

As previously mentioned, the Requirements are mapped back to the 12 Victorian Protective Data Security Standards (**VPDSS**) and 98 elements.

OVIC has mapped the equivalent VPDSS to each Requirement within your PDSP.

This has been included for your reference only.



# Part B – Self-assessment against Requirements

As the Requirement is not overly descriptive, OVIC has offered a tailored **explanation of each Requirement** in both the Class B CT and CoM PDSP.

The explanation outlines the **intent** of the Requirement in plain language.

PART B – Self-assessment against the requirements (mandatory)

Requirement 1

The cemetery trust records how it securely manages its information.

*This requirement maps to Standard 1 of the VPSS An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.*

**Explanation of requirement**

Documentation informs all Class B Cemetery Trust (Class B CT) members (current and future) on the expectations around securely managing Class B CT information.

Proposed completion date for this Requirement (tick one box)

<input type="checkbox"/>	Not commenced (select a proposed completion date)	<input type="checkbox"/>	2026 / 2027
<input type="checkbox"/>	Planned (select a proposed completion date)	<input type="checkbox"/>	2027 / 2028
<input type="checkbox"/>	Partial (select a proposed completion date)	<input type="checkbox"/>	2028 / 2029
<input type="checkbox"/>	Implemented	<input type="checkbox"/>	2029 / 2030
		<input type="checkbox"/>	2030+

OVIC Office of the Victorian Information Commissioner

Class B Cemetery Trust 2026 Protective Data Security Plan | V1.3 Page 6

OFFICIAL



# Part B – Self-assessment against Requirements

The final section to read is the **recommended supporting activity**.

This helps explain how to **implement the Requirement**.

Some of the Requirements are supported by resources and templates.

PART B – Self-assessment against the requirements (mandatory)

**Requirement 1**  
The cemetery trust records how it securely manages its information.

*This requirement maps to Standard 1 of the VPSS: An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.*

**Explanation of requirement**  
Documentation informs all Class B Cemetery Trust (future) on the expectations around securely managing information.

**Recommended supporting activity**  
Trust members discuss and write down their approach to securely managing Class B CT information.  
  
This could be recorded in the form of a simple statement, or for more complex Trusts, it may be recorded in one or more documents.

Action required – complete the below

Current response (tick one box)

<input type="checkbox"/> Not Applicable (must provide rationale)	Rationale for the selection here:	<input type="checkbox"/>
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

OVIC Office of the Victorian Information Commissioner

Class B Cemetery Trust 2026 Protective Data Security Plan | V1.3  
Page 6

OFFICIAL



# Part B – Self-assessment against Requirements

After reading through the Requirement, it is time to provide a response.

Each Requirement contains 3 sections:

- Current response
- Justification if *Not Applicable* was selected
- Proposed completion date

## PART B – Self-assessment against the requirements (mandatory)

### Requirement 1

The cemetery trust records how it securely manages its information.

*This requirement maps to Standard 1 of the VPSSS*

*An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.*

#### Explanation of requirement

Documentation informs all Class B Cemetery Trust (Class B CT) members (current and future) on the expectations around securely managing Class B CT information.

#### Recommended supporting activity

Trust members discuss and write down their approach to securely managing Class B CT information.

This could be recorded in the form of a simple statement, or for more complex Trusts, it may be recorded in one or more documents.

#### Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+



# Part B – Self-assessment against Requirements

The current response should reflect the implementation status of each Requirement at the time of submission.

CoMs and Class B CTs are not expected to have fully implemented each Requirement **in order to submit their PDSP.**

## PART B – Self-assessment against the requirements (mandatory)

### Requirement 1

The cemetery trust records how it securely manages its information.

*This requirement maps to Standard 1 of the VPDS*     *An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.*

#### Explanation of requirement

Documentation informs all Class B Cemetery Trust (Class B CT) members (current and future) on the expectations around securely managing Class B CT information.

#### Recommended supporting activity

Trust members discuss and write down their approach to securely managing Class B CT information.

#### Current response (tick one box)

- Not Applicable (must provide rationale) →
- Not commenced (select a proposed completion date)
- Planned (select a proposed completion date)
- Partial (select a proposed completion date)
- Implemented

...in the form of a simple statement, or for more complex Trusts, it may require more documents.

#### Proposed completion date for this Requirement (tick one box)

- 2026 / 2027
- 2027 / 2028
- 2028 / 2029
- 2029 / 2030
- 2030+



# Part B – Self-assessment against Requirements

Where a Class B CT or a CoM selects **not applicable** as the **current response**, a **rationale must be provided** explaining how this Requirement is not relevant to your trust or committee.

The selection of this status will only apply in rare circumstances.

## PART B – Self-assessment against the requirements (mandatory)

### Requirement 1

The cemetery trust records how it securely manages its information.

This requirement maps to Standard 1 of the VPPDS

An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture

#### Explanation of requirement

Documentation informs all Class B Cemetery Trust (Class B CT) members (current and future) on the expectations around securely managing Class B CT information.

#### Recommended supporting activity

Trust members discuss and write down their approach to securely managing Class B CT information.

This could be recorded in the form of a simple statement, or for more complex Trusts, it may be required in one or more documents.

#### Action required – complete

##### Current response (tick one box)

- Not Applicable (must provide rationale)
- Not commenced (select a proposed completion date)
- Planned (select a proposed completion date)
- Partial (select a proposed completion date)
- Implemented

##### Proposed completion date for this Requirement (tick one box)

- 2026 / 2027
- 2027 / 2028
- 2028 / 2029
- 2029 / 2030
- 2030+

If you select not applicable, you must provide a rationale for the selection here:



# Part B – Self-assessment against Requirements

The **proposed completion** date must be filled out if you select a status of:

- *Not commenced*
- *Planned*
- *Partial*

This date will help OVIC understand how each Class B CT or CoM intends to **prioritise the implementation** of each Requirement.

## PART B – Self-assessment against the requirements (mandatory)

### Requirement 1

The cemetery trust records how it securely manages its information.

This requirement maps to Standard 1 of the ISO 27001.

An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.

#### Explanation of requirement

Documentation informs all Class B Cemetery Trust (Class B CT) members (current and future) on the expectations around securely managing Class B CT information.

#### Recommended supporting activity

Trust members discuss and write down their approach to securely managing Class B CT information.

This could be recorded in...

#### Action required – complete the below

##### Current response (tick one box)

- Not Applicable (must provide rationale) →
- Not commenced (select a proposed completion date)
- Planned (select a proposed completion date)
- Partial (select a proposed completion date)
- Implemented

If you select not applicable, you must provide rationale for the selection here:

##### Proposed completion date for this Requirement (tick one box)

- 2026 / 2027
- 2027 / 2028
- 2028 / 2029
- 2029 / 2030
- 2030+



## Part C – Attestation

The Chairperson, as the public sector body Head of the CoM or Class B CT, must authorise the PDSP before sending a copy to OVIC.

The Attestation **can be signed by an authorised representative**, or by the Chairperson themselves.

**Important!** If an authorised representative is signing the Attestation, please ensure their details are provided in Part A of the PDSP.

### PART C – Attestation (mandatory)

The attestation must be signed by the Chairperson of the Class B Cemetery Trust or their authorised representative (as specified in Part A of this form).

This Protective Data Security Plan is submitted to the Victorian Information Commissioner in accordance with section 89 of the *Privacy and Data Protection Act 2014* (Vic).

I,  \_\_\_\_\_, attest that  \_\_\_\_\_  
(Full Name) (Name of the Class B Cemetery Trust)

- has implemented the 14 requirements, or is in the process of planning and/or implementing these requirements (where applicable), as required by the Victorian Protective Data Security Standards,
- the contents of this PDSP accurately reflect the current information security risks and program of the Class B cemetery trust, and
- I am aware of, and acknowledge, my trust's obligations under Part 4 of the PDP Act.

I am authorised to make this attestation.

Signature: \_\_\_\_\_

Print name: \_\_\_\_\_

Position: \_\_\_\_\_

Date: \_\_\_\_\_

Check this box if more than one Class B cemetery trust is captured by this PDSP.

(Ensure you list the details of the additional Class B cemetery trusts in **Part D of this form**)

**OVIC** Office of the Victorian  
Information Commissioner

Class B Cemetery Trust 2026 Protective Data Security Plan | V1.3

Page 21

OFFICIAL



# Part C – Attestation

The Chairperson, as the public sector body Head of the CoM or Class B CT, must authorise the PDSP before sending a copy to OVIC.

The Attestation **can be signed by an authorised representative**, or by the Chairperson themselves.

If an authorised representative is signing the Attestation, please nominate who this is in Part A of the PDSP.

PART C – Attestation (mandatory)

The attestation must be signed by the Chairperson of the Class B Cemetery Trust or their authorised representative (as specified in Part A of this form)

This Protective Data Security Plan is submitted to the Victorian Information Commissioner in accordance with section 89 of the *Privacy and Data Protection Act 2014* (Vic).

I,  attest that

(Full Name) (Name of the Class B Cemetery Trust)

(required by the Victorian Protective Data Security Standards,

I am authorised to make this attestation. information security risks and program of the Class B cemetery trust, and

nder Part 4 of the PDP Act.

Signature: *J Citizen*

Print name: Jane Citizen

Position: Secretary

Date: 1/08/2026

by this PDSP.

(this form)

**OVIC** Office of the Victorian Information Commissioner Class B Cemetery Trust 2026 Protective Data Security Plan | V1.3  
Page 21

OFFICIAL



# Part D – Reporting on behalf of multiple Committees or Trusts

CoMs or CTs that are submitting on behalf of other CoMs/CTs, must fill out Part D of the form.

The purpose is to minimise administrative overhead by **combining the reporting** of trusts or committees where they have **the same:**

- risk profiles
- types of information
- security practices and
- responses to each of the 14 requirements

Read the How-to Guide for more information.

## PART D – Reporting on behalf of multiple committees of management

The committees of management of Crown land reserves listed in this section have **the same:**

- risk profiles
- types of information
- security practices and
- responses to each of the 14 requirements

and have authorisation from the Chairperson of the committee of management to be included in this submission.

Name of committee of management	Name of the Chairperson	Committee of management phone number <u>and</u> email address	The Chairperson of the committee of management has authorised the submission of this PDSP on their behalf
			<input type="checkbox"/> (check box)
			<input type="checkbox"/> (check box)
			<input type="checkbox"/> (check box)
			<input type="checkbox"/> (check box)
			<input type="checkbox"/> (check box)



## An example

Reading and responding to one of the 14 Requirements



# Reading Requirement 4: An example

## Requirement 4

The committee of management identifies and records information that needs to be accurate and available when used.

*This requirement maps to Standard 2 of the VPDSS An organisation identifies and assesses the security value of public sector information.*

### Explanation of requirement

To ensure CoM information is properly maintained, committee members need to keep up-to-date records. This will help committee members manage the accuracy and availability of the material they hold on behalf of the community.

**Accuracy (integrity)** - If CoM records are inaccurate or incomplete, committee members may find themselves unable to provide the correct information when requested.

*For example* – The CoM is unable to correctly advise on the boundaries of native title on managed land.

**Availability** - If CoM records are unavailable, committee members may find themselves unable to provide information when called upon.

*For example* – A committee member had sole custody of a master CoM record and is no longer able to find it, resulting in advice not being able to be provided.

### Recommended supporting activity

Committee members review their Information Asset Register to identify specific information / records that require careful management to ensure it remains accurate and available.

Members should then update their CoM Information Asset Register, recording which information is essential (i.e. relied upon by committee members for its continued accuracy and availability).

When reviewing the information, consider what would happen if:

- unauthorised adjustments, modifications or changes were made to the information?
- it was unavailable when the information was called upon?

Think about what steps you could take to manage these risks.

### Action required – complete the below

Current response (tick one box)	Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)	<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)	<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)	<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented	<input type="checkbox"/> 2030+

If you select not applicable, you must provide a rationale for the selection here:



# Reading Requirement 4: An example

**Requirement 4**  
The committee of management identifies and records information that needs to be accurate and available when used.

*This requirement maps to Standard 2 of the VPDS: An organisation identifies and assesses the security value of public sector information.*

<p><b>Explanation of requirement</b></p> <p>To ensure CoM information is properly maintained, committee members need to keep up-to-date records. This will help committee members manage the accuracy and availability of the material they hold on behalf of the community.</p> <p><b>Accuracy (integrity)</b> - If CoM records are inaccurate or incomplete, committee members may find themselves unable to provide the correct information when requested.</p> <p><i>For example</i> - The CoM is unable to correctly advise on the boundaries of native title on managed land.</p> <p><b>Availability</b> - If CoM records are unavailable, committee members may find themselves unable to provide information when called upon.</p> <p><i>For example</i> - A committee member had sole custody of a master CoM record and is no longer able to find it, resulting in advice not being able to be provided.</p>	<p><b>Recommended supporting activity</b></p> <p>Committee members review their Information Asset Register to identify specific information / records that require careful management to ensure it remains accurate and available.</p> <p>Members should then update their CoM Information Asset Register, recording which information is essential (i.e. relied upon by committee members for its continued accuracy and availability).</p> <p>When reviewing the information, consider what would happen if:</p> <ul style="list-style-type: none"> <li>unauthorised adjustments, modifications or changes were made to the information?</li> <li>it was unavailable when the information was called upon?</li> </ul> <p>Think about what steps you could take to manage these risks.</p>
--	---

*Actions required - complete the below*

Current response (tick one box)	Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) → <small>if you select not applicable, you must provide a rationale for the selection here.</small>	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)	<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)	<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)	<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented	<input type="checkbox"/> 2030+

Each Requirement relates to a Victorian Protective Data Security Standard.

Because they have been **simplified**, some Requirements will have **multiple aspects** to them. It is important to carefully read the Requirement to ensure each aspect is addressed.

Using Requirement 4 as an example, we have highlighted the four aspects that you need to carefully consider.

## Requirement 4

The committee of management **identifies** and **records** information that needs to be **accurate** and **available** when used.





# Reading Requirement 4: An example

## Explanation of requirement

To ensure CoM information is properly maintained, committee members need to keep up-to-date records. This will help committee members manage the accuracy and availability of the material they hold on behalf of the community.

**Accuracy (integrity)** - If CoM records are inaccurate or incomplete, committee members may find themselves unable to provide the correct information when requested.

*For example* – The CoM is unable to correctly advise on the boundaries of native title on managed land.

**Availability** - If CoM records are unavailable, committee members may find themselves unable to provide information when called upon.

*For example* – A committee member had sole custody of a master CoM record and is no longer able to find it, resulting in advice not being able to be provided.

Requirement 4 is about ensuring information is:

- **accurate** and
- **available** when needed.

In this explanation, we have described two scenarios of how not having accurate or available records could impact the daily operations of a committee or trust.

**Requirement 4**  
The committee of management identifies and records information that needs to be accurate and available when used.

This requirement maps to Standard 2 of the VPOSI: An organisation identifies and assesses the security value of public sector information.

**Explanation of requirement**

To ensure CoM information is properly maintained, committee members need to keep up-to-date records. This will help committee members manage the accuracy and availability of the material they hold on behalf of the community.

**Accuracy (integrity)** - If CoM records are inaccurate or incomplete, committee members may find themselves unable to provide the correct information when requested.

*For example* – The CoM is unable to correctly advise on the boundaries of native title on managed land.

**Availability** - If CoM records are unavailable, committee members may find themselves unable to provide information when called upon.

*For example* – A committee member had sole custody of a master CoM record and is no longer able to find it, resulting in advice not being able to be provided.

**Recommended supporting activity**

Committee members review their Information Asset Register to identify specific information / records that require careful management to ensure it remains accurate and available.

Members should then update their CoM Information Asset Register, recording which information is essential (i.e. relied upon by committee members for its continued accuracy and availability).

When reviewing the information, consider what would happen if:

- unauthorised adjustments, modifications or changes were made to the information?
- it was unavailable when the information was called upon?

Think about what steps you could take to manage these risks.

Current response (see note)	Response due to the VPOSI	Response due to the Information Asset Register
<input type="checkbox"/> Not Applicable (must provide reasons) →	<input type="checkbox"/> If you select not applicable, you must provide a response for this section here.	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Partial (select a proposed completion date)		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+

## Example 1:

Because a CoM has **not yet identified** and **recorded** the boundaries of native title on managed land, they are **unable to accurately provide this information** when needed.



# Reading Requirement 4: An example

## Explanation of requirement

To ensure CoM information is properly maintained, committee members need to keep up-to-date records. This will help committee members manage the accuracy and availability of the material they hold on behalf of the community.

**Accuracy (integrity)** - If CoM records are inaccurate or incomplete, committee members may find themselves unable to provide the correct information when requested.

*For example* – The CoM is unable to correctly advise on the boundaries of native title on managed land.

**Availability** - If CoM records are unavailable, committee members may find themselves unable to provide information when called upon.

*For example* – A committee member had sole custody of a master CoM record and is no longer able to find it, resulting in advice not being able to be provided.

Requirement 4 is about ensuring information is:

- **accurate** and
- **available** when needed.

In this explanation, we have described two scenarios of how not having accurate or available records could impact the daily operations of a committee or trust.

**Requirement 4**  
The committee of management identifies and records information that needs to be accurate and available when used.

This requirement maps to Standard 2 of the VPOSS: An organisation identifies and assesses the security value of public sector information.

<p><b>Explanation of requirement</b></p> <p>To ensure CoM information is properly maintained, committee members need to keep up-to-date records. This will help committee members manage the accuracy and availability of the material they hold on behalf of the community.</p> <p><b>Accuracy (integrity)</b> - If CoM records are inaccurate or incomplete, committee members may find themselves unable to provide the correct information when requested.</p> <p><i>For example</i> – The CoM is unable to correctly advise on the boundaries of native title on managed land.</p> <p><b>Availability</b> - If CoM records are unavailable, committee members may find themselves unable to provide information when called upon.</p> <p><i>For example</i> – A committee member had sole custody of a master CoM record and is no longer able to find it, resulting in advice not being able to be provided.</p>	<p><b>Recommended supporting activity</b></p> <p>Committee members review their Information Asset Register to identify specific information records that require careful management to ensure it remains accurate and available.</p> <p>Members should then update their CoM Information Asset Register, recording which information is essential (i.e. relied upon by committee members for its continued accuracy and availability).</p> <p>When reviewing the information, consider what would happen if:</p> <ul style="list-style-type: none"> <li>unauthorised adjustments, modifications or changes were made to the information?</li> <li>it was unavailable when the information was called upon?</li> </ul> <p>Think about what steps you could take to manage these risks.</p>
--	---

Current regulated trust use base	Information Asset Register (IAR) use base
<input type="checkbox"/> Not Applicable (trust provides advisory) →	If you select not applicable, you must provide a response for this question base.
<input type="checkbox"/> Not completed (select a proposed completion date)	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Planned (select a proposed completion date)	<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Partial (select a proposed completion date)	<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Implemented	<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented	<input type="checkbox"/> 2030+

## Example 2:

Because a CoM has **not yet identified** and **recorded** who has **custody** of a master record, other CoM members are **unable to locate the record**, rendering it unavailable.



# Reading Requirement 4: An example

## Recommended supporting activity

Committee members review their Information Asset Register to identify specific information / records that require careful management to ensure it remains accurate and available.

Members should then update their CoM Information Asset Register, recording which information is essential (i.e. relied upon by committee members for its continued accuracy and availability).

When reviewing the information, consider what would happen if:

- unauthorised adjustments, modifications or changes were made to the information?
- it was unavailable when the information was called upon?

Think about what steps you could take to manage these risks.

Consider how the supporting activity can assist your Committee or Trust to meet the Requirement.

This particular activity suggests committees / trusts **develop** and **maintain** an **Information Asset Register** to help identify the different information it manages.

To support you in this, OVIC has developed a templated register specifically for CoMs and Class B CTs. If you wish to use this templated register, you can download a digital or printable copy from our website:

**Requirement 4**  
The committee of management identifies and records information that needs to be accurate and available when used.

This requirement maps to Standard 2 of the VPOSS: An organisation identifies and assesses the security value of public sector information.

Explanation of requirement	Recommended supporting activity
<p>To ensure CoM information is properly maintained, committee members need to keep up-to-date records. This will help committee members manage the accuracy and availability of the material they hold on behalf of the community.</p> <p><b>Accuracy (integrity)</b> - If CoM records are inaccurate or incomplete, committee members may find themselves unable to provide the correct information when requested.</p> <p><i>For example - The CoM is unable to accurately advise on the boundaries of native title on managed land.</i></p> <p><b>Availability</b> - If CoM records are unavailable, committee members may find themselves unable to provide information when called upon.</p> <p><i>For example - A committee member had sole custody of a master CoM record and is no longer able to find it, resulting in advice not being able to be provided.</i></p>	<p>Committee members review their Information Asset Register to identify specific information / records that require careful management to ensure it remains accurate and available.</p> <p>Members should then update their CoM Information Asset Register, recording which information is essential (i.e. relied upon by committee members for its continued accuracy and availability).</p> <p>When reviewing the information, consider what would happen if:</p> <ul style="list-style-type: none"> <li>• unauthorised adjustments, modifications or changes were made to the information?</li> <li>• it was unavailable when the information was called upon?</li> </ul> <p>Think about what steps you could take to manage these risks.</p>

Current registered trust use base	When last registered trust use base was updated
<input type="checkbox"/> Not Applicable (trust provides services) →	If you select not applicable, you must provide a date for this version base.
<input type="checkbox"/> Not commenced (select a proposed completion date)	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Planned (select a proposed completion date)	<input type="checkbox"/> 2027 / 2028
<input type="checkbox"/> Partial (select a proposed completion date)	<input type="checkbox"/> 2028 / 2029
<input type="checkbox"/> Implemented	<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented	<input type="checkbox"/> 2030+



## Information Asset Register template

<https://go.vic.gov.au/4s2mwJa>



## How-To Guide for the Information Asset Register

<https://go.vic.gov.au/3MQFsvi>



# Responding to Requirement 4: An example

## Selecting the most appropriate 'current response'

Assess the status of your committee or trust's implementation of Requirement 4 using the descriptions offered.

<b>Not applicable</b>	This requirement is <b>deemed not applicable</b> to the committee or trust, and it <b>documents why</b> .
<b>Not commenced</b>	The requirement is applicable; however, <b>no work has started or been planned</b> at the current time.
<b>Planned</b>	No work has been started but a <b>plan is in place</b> to meet this requirement.
<b>Partial</b>	<b>Work is underway</b> to meet this requirement but is not yet fully implemented.
<b>Implemented</b>	The requirement is <b>fully implemented</b> , and the supporting activities are being actively managed.

In this example, the committee or trust has **completed some aspects of the Requirement, but hasn't finalised all components**.

Work is underway on filling in an Information Asset Register (IAR) but **this has not been completed just yet**.

Action required – complete the below

Current response (tick one box)

- Not Applicable (must provide rationale) →
- Not commenced (select a proposed completion date)
- Planned (select a proposed completion date)
- Partial (select a proposed completion date)
- Implemented



## A word on *not applicable* as a response

Whilst not relevant to the working example discussed in today's session, there will times where a CoM or Class B CT selects the *current response* as *not applicable*. In this scenario a rationale must be provided in the corresponding box outlining why this is the case.

### Action required – complete the below

Current response (tick one box)

Not Applicable (must provide rationale) →

Not commenced (select a proposed completion date)

Planned (select a proposed completion date)

Partial (select a proposed completion date)

Implemented

**Note:** A rationale does not need to be supplied if a CoM or Class B CT selects any other *current response*.

A rationale is only required where *not applicable* is selected.

If you select not applicable, you must provide a rationale for the selection here:

The committee / trust does not ...



## Responding to Requirement 4: An example

### Determining the proposed completion date

After reading through the Requirement, your committee / trust will have determined the most appropriate current response. This response should reflect how the Class B CT or CoM is tracking against addressing and implementing each aspect of the Requirement.

Where you have selected:

- *Not commenced*
- *Planned, or*
- *Partial*

as the *current response*, you must now nominate a proposed completion date.

Tick the relevant box next to the most appropriate completion date. The date nominated should reflect when the committee / trust thinks all aspects of the Requirement are likely to be finalised.

**Remember:** You do not need to select a proposed completion date if you have selected a current response of *implemented* or *not applicable*.

In this example, we have said the CoM / Trust has **partially** implemented Requirement 4, with a proposed date of having this **fully implemented and maintained** by 2027/2028.

#### Proposed completion date for this Requirement (tick one box)

- |                                     |             |
|-------------------------------------|-------------|
| <input type="checkbox"/>            | 2026 / 2027 |
| <input checked="" type="checkbox"/> | 2027 / 2028 |
| <input type="checkbox"/>            | 2028 / 2029 |
| <input type="checkbox"/>            | 2029 / 2030 |
| <input type="checkbox"/>            | 2030+       |



# Finalised response for Requirement 4: An example

## Requirement 4

The committee of management identifies and records information that needs to be accurate and available when used.

*This requirement maps to Standard 2 of the VPDSS An organisation identifies and assesses the security value of public sector information.*

### Explanation of requirement

To ensure CoM information is properly maintained, committee members need to keep up-to-date records. This will help committee members manage the accuracy and availability of the material they hold on behalf of the community.

**Accuracy (integrity)** - If CoM records are inaccurate or incomplete, committee members may find themselves unable to provide the correct information when requested.

*For example* – The CoM is unable to correctly advise on the boundaries of native title on managed land.

**Availability** - If CoM records are unavailable, committee members may find themselves unable to provide information when called upon.

*For example* – A committee member had sole custody of a master CoM record and is no longer able to find it, resulting in advice not being able to be provided.

### Recommended supporting activity

Committee members review their Information Asset Register to identify specific information / records that require careful management to ensure it remains accurate and available.

Members should then update their CoM Information Asset Register, recording which information is essential (i.e. relied upon by committee members for its continued accuracy and availability).

When reviewing the information, consider what would happen if:

- unauthorised adjustments, modifications or changes were made to the information?
- it was unavailable when the information was called upon?

Think about what steps you could take to manage these risks.

### Action required – complete the below

Current response (tick one box)		Proposed completion date for this Requirement (tick one box)
<input type="checkbox"/> Not Applicable (must provide rationale) →	If you select not applicable, you <u>must</u> provide a rationale for the selection here:	<input type="checkbox"/> 2026 / 2027
<input type="checkbox"/> Not commenced (select a proposed completion date)		<input checked="" type="checkbox"/> 2027 / 2028 ←
<input type="checkbox"/> Planned (select a proposed completion date)		<input type="checkbox"/> 2028 / 2029
<input checked="" type="checkbox"/> Partial (select a proposed completion date) ←		<input type="checkbox"/> 2029 / 2030
<input type="checkbox"/> Implemented		<input type="checkbox"/> 2030+



## Submission steps and information



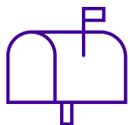
# How to submit the PDSP to OVIC

Once you have completed the PDSP form and signed the Attestation, you need to supply a copy to OVIC.

This can be done via email or by post.



**Email** a copy of your PDSP to OVIC's Information Security Unit at [security@ovic.vic.gov.au](mailto:security@ovic.vic.gov.au)



**Mail** a copy of your PDSP using the following details:

**Attention:** Information Security Unit  
 OVIC PO Box 24274  
 Melbourne Victoria 3001

Submit a PDSP to OVIC by  
**31 August 2026**

Ensure it is signed by the chairperson or an authorised representative



**Remember:** It is good practice to keep a record and copies of any forms (including the PDSP) that you submit to OVIC.

Jan

Feb

Mar

Apr

May

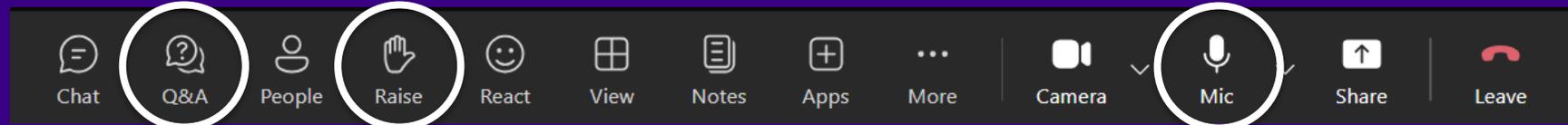
Jun

Jul

Aug



# Questions?



Click here for the Q&A feature to open. Type your question here.

Click this button to raise your hand to verbally ask a question.

When called upon, click this button to turn on your mic.



Have your say on this information session – <https://forms.office.com/r/dkPKffjgit>



# Who can I talk to?



## Office of the Victorian Information Commissioner

We can answer questions about the resources and PDSP.  
Email OVIC:



[security@ovic.vic.gov.au](mailto:security@ovic.vic.gov.au)



## Department of Energy, Environment and Climate Action

For Committees of Management, visit DEECA's [Committees of management](#) page for more guidance or email:



[voluntarycommittees@deeca.vic.gov.au](mailto:voluntarycommittees@deeca.vic.gov.au)



## Department of Health

For Class B cemetery trusts, visit the [Department of Health Cemetery Sector Governance Support](#) page for more guidance or email:



[cemeteries@health.vic.gov.au](mailto:cemeteries@health.vic.gov.au)



## Find out more


About us    For organisations & agencies

### Committees of Management of Crown Land Reserve stakeholders

In Victoria there are over 1,500 Crown land reserves (also referred to as public land reserves) managed by approximately 1,125 voluntary committees of management (CoMs) appointed as land managers under the *Crown Land (Reserves) Management Act 1978 (Vic) (CLRA)*.


About us    For organisations & agencies

### Class B Cemetery Trust stakeholders

In Victoria there are over 400 Class B Cemetery Trusts (Class B CTs) managed by community members, often in a voluntary capacity. These Class B CTs are public boards that manage public cemeteries and deliver services with care and compassion.

Visit the OVIC website to download the:

- *2026 Protective Data Security Plan* for either Class B CTs or Committees of Management
- Corresponding *How to: A Guide to completing a PDSP* for either Class B CTs or Committees of Management

You can find all relevant guidance material and resources for:

- Committees of Management here: <https://go.vic.gov.au/4pScREm>
- Class B Cemetery Trusts here: <https://go.vic.gov.au/3VFX4KD>



Have your say on this information session – <https://forms.office.com/r/dkPKffjgit>



## Final thoughts

Anthony Corso

*Acting Privacy and Data Protection, Deputy Commissioner*



Have your say on this information session –  
<https://forms.office.com/r/dkPKffjgit>

**OVIC**  
[www.ovic.vic.gov.au](http://www.ovic.vic.gov.au)