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**

Contents

Document Details

Version	Publish date	Amendments in this version
1.0	July 2020	Initial version for Cemetery Trusts
1.1	January 2022	2022 Class B Cemetery Trust PDSP form has been released with amendments
1.2	December 2023	2024 Class B Cemetery Trust PDSP form has been released with amendments
1.3	December 2025	2026 Class B Cemetery Trust PDSP form has been released with amendments including: - refreshed design and readability - addition of mapping the requirements to the Victorian Protective Data Security Standards - inclusion of Information Security Obligations from Part 4 of the PDP Act - addition of an optional free text commentary field - updated attestation

How will the information in the PDSP be used and managed?

In-line with OVIC's functions under the PDP Act, content from PDSP submissions may form the basis of reporting back to organisations and the Victorian Government including the Victorian Government Chief Information Security Officer.

OVIC will collect some personal information as part of the PDSP form including the name and contact details of the public sector body Head and nominated contact (Information Security Lead). OVIC will use this information to communicate with these contacts about the PDSP, broader security initiatives and activities, distributing information security-related content, or collecting feedback.

OVIC will not disclose personal information without consent, except where required to do so by law. For more information about how OVIC handles personal information, please see OVIC's Privacy Policy.

The information provided in the PDSP will be managed in accordance with the protective marking assigned. The contents of the PDSP are exempt from the *Freedom of Information Act 1982* (Vic).

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[1] 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.

[1] For the full list of requirements, see section 88 and 89 of the PDP Act.

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			

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.

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)
☐	Not Applicable (must provide rationale) →	If you select not applicable, you must provide a rationale for the selection here:	☐ 2026 / 2027
☐	Not commenced (select a proposed completion date)		☐ 2027 / 2028
☐	Planned (select a proposed completion date)		☐ 2028 / 2029
☐	Partial (select a proposed completion date)		☐ 2029 / 2030
☐	Implemented		☐ 2030+

Requirement 2

The cemetery trust identifies and records the different types of information it manages.

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

Explanation of requirement

Class B CTs manage different kinds of information, such as:

- right of interment and interment registers
- meeting agendas and minutes
- correspondence
- financial statements, invoices, and receipts
- policies and procedures
- instruments of delegation
- employee contracts
- maps

Sometimes these are kept in paper or electronic form.

Identifying and documenting the different types of information that trust members manage helps build community confidence.

Recommended supporting activity

Trust members discuss the various information types managed by the Class B CT. This will help the trust identify the different information it manages.

Members should then create a summarised record of these information types, noting these down in either a hard copy or electronic (digital) format.

OVIC has developed a template for Class B CTs to document these actions. This template is referred to as an Information Asset Register. Class B CTs are encouraged to use this template to identify and record their information.

- A copy of this template is available on the OVIC website. Please navigate to https://ovic.vic.gov.au/information-security/agency-reporting-obligations/class-b-cemetery-trust-stakeholders/ where you can download this resource.
- If you require assistance please contact OVIC at security@ovic.vic.gov.au or 1300 006 842.

Action required – complete the below

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

Requirement 3

The cemetery trust identifies and records sensitive information it manages.

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 Cemetery Trust information is properly protected, members need to identify and record material that is sensitive in nature. This will help Cemetery Trust members maintain the confidentially of the material they are managing on behalf of the community.

For instance, some information types may have more sensitive components to them, e.g. interment records may have components that trust members are authorised to disclose, but there may be other components of these same interment records that need to remain confidential – i.e. details of next of kin, addresses, cause of death, credit card details etc.

Recommended supporting activity

Trust members review the Class B CT Information Asset Register to identify specific information types (contents) that are considered confidential or sensitive (i.e. not for public distribution).

Members should then update the Class B CT Information Asset Register, recording which information has sensitive components associated with it.

When reviewing your information, consider what would happen if:

- an unauthorised person accessed this material, or
- it was disclosed to someone who wasn't supposed to see or hear it?

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)
☐	Not Applicable *(*must provide rationale) →	If you select not applicable, you must provide a rationale for the selection here:	☐ 2026 / 2027
☐	Not commenced (select a proposed completion date)		☐ 2027 / 2028
☐	Planned (select a proposed completion date)		☐ 2028 / 2029
☐	Partial (select a proposed completion date)		☐ 2029 / 2030
☐	Implemented		☐ 2030+

Requirement 4

The cemetery trust 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 Class B CT information is properly maintained, trust members need to keep up-to-date records. This will help trust members manage the accuracy and availability of the material they hold on behalf of the community.

Accuracy (integrity) - If Class B CT records are inaccurate or incomplete, trust members may find themselves unable to provide the correct information when requested.

> *For example* – The Class B CT is unable to correctly advise who was interred in a particular plot.

Availability - If Class B CT records are unavailable, trust members may find themselves unable to provide information when called upon.

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

Recommended supporting activity

Trust 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 Class B CT Information Asset Register, recording which information is essential (i.e. relied upon by trust 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)
☐	Not Applicable (must provide rationale) →	If you select not applicable, you must provide a rationale for the selection here:	☐ 2026 / 2027
☐	Not commenced (select a proposed completion date)		☐ 2027 / 2028
☐	Planned (select a proposed completion date)		☐ 2028 / 2029
☐	Partial (select a proposed completion date)		☐ 2029 / 2030
☐	Implemented		☐ 2030+

Requirement 5

The cemetery trust documents any information security risks relating to the management of its information.

This requirement maps to Standard 3 of the VPDSS

An organisation utilises its risk management framework to undertake a Security Risk Profile Assessment to manage information security risks.

Explanation of requirement

The Class B CT documents information security risks associated with the Class B CT material they manage on behalf of the community.

By understanding and documenting these risks, the Class B CT can prioritise its efforts and resources.

Recommended supporting activity

Trust members may already have a register of risks for their Class B CT, stored in paper or electronic (digital) form. This activity supports existing recommendations set out in the DH Cemetery Trust Manual.

Requirement 5 calls on trust members to simply update this existing register with any information security risks identified in your discussions.

> *For example* – An information security risk that may be recorded in your register could be *"The risk of Cemetery Trust documents being destroyed, caused by a fire (no backups available), resulting in lack of confidence from the local community in the management of the cemetery trust".*

The Class B CT may seek to manage this risk by creating copies of its records and storing these copies away from originals.

Action required – complete the below

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

Requirement 6

The cemetery trust validates who (people) and what (systems) have direct access to its information.

This requirement maps to Standard 4 of the VPDSS — *An organisation establishes, implements and maintains an access management process for controlling access to public sector information.*

Explanation of requirement

The Class B CT ensures only the right people and systems are granted direct access to Class B CT information, when and where appropriate. The *right*:

- *people* may include, but are not limited to, authorised employees or volunteers performing certain roles for the Class B CT, individuals from neighbouring cemetery trusts, or private organisations providing support or assistance to the trust.
- *systems* may include, but are not limited to, internal or external IT systems that have been authorised to process and/or store Class B CT information (e.g. computer, server, email system).

Class B CTs are expected to 'validate' (confirm / approve) the legitimacy of these people and systems before granting direct access to Class B CT information. This includes external organisations and/or systems. Members of the Class B CTs should clarify how the trust's information will be used by these individuals and/or systems.

Recommended supporting activity

Trust members discuss, verify and document who (people or organisations) and what (systems – if any) should be granted access to cemetery trust information. For example, consider:

- which Class B CT roles are authorised to directly access certain information, and which roles should be restricted from accessing the same material?
- how the Class B CT will validate requests from third parties, such as community members, private industry groups and/or systems, taking into account whether the requests for access are legitimate and permitted by law /regulation?

Action required – complete the below

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

Requirement 7

The cemetery trust documents the roles and responsibilities for those managing trust information.

This requirement maps to Standard 5 of the VPDSS *An organisation ensures all persons understand their responsibilities to protect public sector information.*

Explanation of requirement

The Class B CT:

- has documented expectations around the handling and management of trust information.
- ensures everyone understands their roles and responsibilities when managing cemetery trust information on behalf of the community.

Recommended supporting activity

Class B CT members discuss and document the roles and responsibilities of personnel that handle and manage cemetery trust information. Consider:

- what roles are responsible for what types of information
- whether Class B CT members know what information they are allowed to disclose, and in what circumstances
- how the Class B CT will communicate these expectations to personnel.

Personnel may include:

- volunteers
- individual trust members
- staff
- third parties (sub-contractors).

Action required – complete the below

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

Requirement 8

The cemetery trust manages any compromises (incidents) to its information.

This requirement maps to Standard 6 of the VPDSS

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

Explanation of requirement

The Class B CT has documented expectations around the handling and management of situations where trust information has been compromised.

To help reduce the impact of an information security incident (i.e. where trust information has been adversely affected) Class B CTs should refer to a documented plan.

Information security incident examples can include scenarios where:

- sensitive information has been mistakenly released to a member of the public via an enquiry (e.g. giving out contact details) where this wasn't permitted by relevant laws or regulations
- trust information has been stolen, lost or damaged.

Recommended supporting activity

Trust members discuss and document how they will deal with a variety of information security incidents.

It is important to think through different scenarios and have a plan in place to manage incidents that have the potential to affect the confidentiality, integrity and/or availability of cemetery trust information. For example, in the event of an incident think about:

- What steps would you need to take?
- Who would you notify of the incident? E.g., OVIC, DH, Victoria Police
- Who will manage the incident?
- Who can you turn to for help?
- Where is the cemetery trust's incident management plan?

Action required – complete the below

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

Requirement 9

The cemetery trust documents how it intends to protect its information in the event of a disaster.

This requirement maps to Standard 7 of the VPDSS *An organisation embeds information security continuity in its business continuity and disaster recovery processes and plans.*

Explanation of requirement

The Class B CT has documented expectations around the handling and ongoing management of cemetery trust information in situations where the operations of the trust have been adversely impacted. Examples of this could include:

- a natural disaster such as fire or flood
- system outages
- unplanned liquidation or discontinuation of a service offered by a third party.

Recommended supporting activity

Trust members discuss and document how the Class B CT would continue to keep its information secure, if the operations of the trust were severely undermined or impacted. Take into account information stored in both hard copy and electronic (digital) format.

For example:

- have trust members considered creating secure copies or backups of the trust's information?
- where are these copies securely stored? Are they stored away from the normal office/home environment, separate from the originals?
- would these copies be available following an accident or disaster?

Action required – complete the below

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

Requirement 10

The cemetery trust documents how non-trust members access and/or use its information in a secure way.

This requirement maps to Standard 8 of the VPDSS *An organisation ensures that third parties securely collect, hold, manage, use, disclose or transfer public sector information.*

Explanation of requirement

The Class B CT has documented its expectations around the secure handling and ongoing management of trust information by non-trust members, including establishing clear expectations around what is required of them when accessing or using its information.

Recommended supporting activity

Trust members discuss and document:

- who is authorised to access the trust information?
  (e.g., DH, Victoria Police, Local Council, members of the public)
- in what circumstances this access is permitted / authorised
- how the information will be provided to non-trust members
- the various protections required when sharing this information.

Action required – complete the below

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

Requirement 11

The cemetery trust notifies OVIC of any compromises (incidents) to its information.

This requirement maps to Standard 9 of the VPDSS

An organisation regularly assesses its implementation of the Victorian Protective Data Security Standards (VPDSS) and reports to the Office of the Victorian Information Commissioner (OVIC).

Explanation of requirement

The Class B CT ensures OVIC is made aware of any issues impacting the security of its information.

To ensure the continued security of Class B CT information, the confidentiality, integrity and/or availability of this material must be maintained. If any of these attributes are ever compromised, an information security incident may have occurred.

An example of an information security incident may be where:

- a trust member mistakenly discloses sensitive information (confidentiality)
- trust records have been altered to misrepresent burial plots (integrity)
- an asset register goes missing (lack of availability)

Recommended supporting activity

Trust members discuss and document:

- potential types of incidents that may impact Class B CT information
- who would notify OVIC and in what circumstances
- how they would notify OVIC.

Remember, if the confidentiality, integrity and/or availability of Class B CT information has been compromised, it is likely that an information security incident may have occurred.

If you require assistance, please contact OVIC.

Action required – complete the below

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

Requirement 12

The cemetery trust members are checked prior to, and throughout, their appointment.

This requirement maps to Standard 10 of the VPDSS

An organisation establishes, implements and maintains personnel security controls addressing all persons continuing eligibility and suitability to access public sector information.

Explanation of requirement

The Class B CT ensures that its members are eligible and suitable to manage cemetery trust information.

Class B CT are responsible for conducting interviews and referee checks prior to endorsing applications for appointment. In addition to this, the Department of Health (**DH**) is responsible for undertaking probity checks of applicants endorsed by the trust.

Cemetery trusts should ensure members remain eligible and suitable to access, use and handle trust information on an ongoing basis. This is particularly relevant for lifetime members as they are not required to go through the application process every 5 years. If personal circumstances of trust members change, it is the responsibility of the trust to manage these.

Recommended supporting activity

Trust members discuss and document the requirements for validating the eligibility and suitability of individuals prior to, and during, their appointment. Trust members refer to this documentation when conducting checks.

The cemetery trust will notify DH if it believes a member has become unsuitable to continue as a trust member.

Action required – complete the below

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

Requirement 13

The cemetery trust securely maintains computer systems that process and/or store its information.

This requirement maps to Standard 11 of the VPDSS *An organisation establishes, implements and maintains Information Communications Technology security controls.*

Explanation of requirement

If the Class B CT uses computer systems / devices to process or store trust information, trust members must ensure these systems/devices are secure.

This requirement extends to arrangements where the Class B CT is using a third party (contracted service provider) to help administer trust operations on its behalf.

Where a third party uses a computer system or device to process/store cemetery trust information, the trust must be comfortable with their security arrangements.

- Systems may include cloud-based programs run by a vendor, or programs managed on a local desktop computer or laptop.
- Devices can include desktop computers, laptops, smart phones, tablets, iPads, etc.

Only select "not applicable" if the trust is not using computer systems or devices to process and/or store trust information.

Recommended supporting activity

Trust members discuss and document the requirements for ensuring any computer systems (including cloud-based systems) or devices processing/storing cemetery trust information are secure.

Trust members may consider:

- updating software on any systems / devices
- using strong passwords
- backing up systems / devices
- using anti-virus software
- being mindful of any links members may click on (e.g., phishing attempts, scams.)
- using multi-factor authentication methods (where offered)

Action required – complete the below

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

Requirement 14

The cemetery trust maintains its facilities, equipment and services that help securely manage its information and systems.

This requirement maps to Standard 12 of the VPDSS

An organisation establishes, implements and maintains physical security controls addressing facilities, equipment and services.

Explanation of requirement

The Class B CT ensures its hardcopy and softcopy information is physically protected in various forms. This includes using physical security controls for any:

- facilities (buildings) where cemetery trust information or systems are handled or stored
- equipment used to store or manage cemetery trust information or systems
- services that help monitor or protect locations or facilities where cemetery trust information or systems are stored.

Recommended supporting activity

Trust members discuss and document the requirements for maintaining physical security controls designed to protect cemetery trust information. Physical measures may include:

- facilities – e.g., locks on doors, alarms
- equipment – e.g., types of containers that are used to store information, such as locked cabinets, safes, protective containers or boxes (to avoid water or insect damage)
- services – e.g., security guard, monitoring companies where applicable.

Action required – complete the below

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

Commentary section (optional)

Please use the space below if you wish to provide any additional information or commentary on the Class B Cemetery Trust, or the 14 requirements.

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**)*

PART D – Reporting on behalf of multiple cemetery trusts

The Class B Cemetery Trusts 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 below Class B Cemetery Trusts to be included in this submission.

Name of the Class B Cemetery Trust	Name of the Chairperson	Class B Cemetery Trust phone number and email address	The Chairperson of the Class B Cemetery Trust has authorised the submission of this PDSP on their behalf
			☐ *(check box)*
			☐ *(check box)*
			☐ *(check box)*
			☐ *(check box)*
			☐ *(check box)*