Submission No 11

INQUIRY INTO FRAUD AND CORRUPTION CONTROL IN LOCAL GOVERNMENT: A FOLLOW UP OF TWO AUDITOR-GENERAL REPORTS

Name: Office of the Victorian Information Commissioner

Date Received: 14 March 2025

Submission to the Public Accounts and Estimates Committee's Inquiry into fraud and corruption control in local government

Introduction

Councils hold a range of personal and sensitive information about Victorians – information about ratepayers and pet owners, information relating to planning decisions, details of complaints, and information associated with delivering community services such waste management, libraries, maternal and child health and kindergartens. Local government information and systems are also part of a broader information ecosystem shared by the whole of the Victorian Government. Therefore, the same mandatory information security protections should apply to local government information and systems that apply to Victorian public sector (**VPS**) information and systems.

Overview of existing legislative and regulatory frameworks

Part 3 of the PDP Act

Part 3 of the PDP Act establishes the Information Privacy Principles (**IPPs**). The IPPs outline 10 principles that govern the collection, use, disclosure, handling, security and storage of personal information. These principles apply to VPS organisations including local councils. Section 13 of the PDP Act outlines the organisations to which Part 3 applies.

Part 4 of the PDP Act

Part 4 of the PDP Act enables the development of the Victorian Protective Data Security Framework (**VPDSF**) and the Victorian Protective Data Security Standards (**VPDSS**).[1] Part 4 also requires organisations to submit a Protective Data Security Plan (**PDSP**) to OVIC and develop a Security Risk Profile Assessment (**SRPA**).[2] Organisations captured by Part 4 are required to conduct their own monitoring and assurance activities to track their exposure to information security risks, and assess and triage those risks.

Local councils are excluded from Part 4 of the PDP Act.[3] This means that they are not subject to the obligations arising from Part 4 including the VPDSF and VPDSS. However, local councils are also often appointed as Committees of Management for Crown land reserves and as trustees of Cemetery

[1] See sections 85 and 86 of the PDP Act. For more information on the VPDSF see https://ovic.vic.gov.au/information-security/framework-vpdsf/. For more information on the VPDSS see https://ovic.vic.gov.au/information-security/standards/

[2] See section 89 of the PDP Act. For more information on PDSPs, see https://ovic.vic.gov.au/information-security/agency-reporting-obligations/#protective-data-security-plan.

[3] See section 84(2)(a) of the PDP Act.

Trusts. Those bodies are subject to Part 4 of the PDP Act, and therefore any information and systems that local councils use in exercising those functions will be captured.[4]

Victorian Protective Data Security Framework and Standards

The VPDSF provides direction to VPS organisations on their data security obligations. It builds security risk management capability and maturity through the use of established risk management principles and guidelines. The VPDSF is accompanied by the 12 VPDSS.

The VPDSS establish high level mandatory requirements to protect public sector information and systems across all security domains – that is, governance, personnel, physical, cyber and information security. The VPDSS controls help to mitigate fraud and corruption risks by compelling organisations to develop an effective information security program. The VPDSS are accompanied by VPDSS Implementation Guidance, which includes 98 supporting VPDSS elements.[5] These elements provide a suite of controls on which organisations can base their information security programs.

Information Security Incident Notification Scheme

One of the elements outlined in the VPDSS Implementation Guidance (E9.010) provides the foundation for the Information Security Incident Notification Scheme (**ISINS**).[6] This voluntary scheme sets an expectation that organisations subject to Part 4 notify OVIC of incidents that have an adverse impact on the confidentiality, integrity or availability of public sector information with a business impact level of 2 or higher.

Protective Data Security Plans and Security Risk Profile Assessments

Organisations that identify and manage risks enhance their capability to respond to information security incidents and recover from adverse impacts arising from those incidents. Part 4 of the PDP Act requires organisations to develop a PDSP and undertake an SRPA to prioritise information security risks to provide efficient, effective deployment of security controls.

Regulated organisations are required to submit a PDSP to OVIC every two years or sooner in the event of a significant change. The PDSP and SRPA act as tools that:

- advise OVIC of the organisation's self-assessed maturity and implementation status of the VPDSS
- articulate the organisation's security risk profile
- in the case of PDSPs, compel public sector body Heads to attest to the implementation activities.

[4] For more information on the instances in which Part 4 of the PDP Act applies to local government authorities, see https://ovic.vic.gov.au/resource/local-government-authorities-information-security-obligations/.
[5] See https://ovic.vic.gov.au/wp-content/uploads/2024/02/VPDSS-V2.0-Implementation-Guidance-V2.3-web-version.pdf#page=10&zoom=100,92,113.
[6] See https://ovic.vic.gov.au/information-security/ovic-information-security-incident-notification-scheme/.

OVIC publishes statistics and general insights drawn from PDSPs.[7] These insights and observations include general trends and themes observed across the VPS, a comparison of whole of Victorian Government vs. portfolio reporting, and offers suggested next steps for VPS organisations and OVIC. These insights act as a further input for the identification of security risk trends and potential mitigation strategies.

Recent trends in fraud and corruption within local government relating to information security and administrative systems

The following sections provide an overview of the trends OVIC is observing in relation to each of the three oversight areas – privacy, information security and freedom of information (**FOI**).

Privacy

OVIC's Privacy Guidance and Dispute Resolution Unit conciliates complaints made against councils where there has been an alleged failure to uphold their privacy obligations under Part 3 of the PDP Act. In the 2024-25 financial year to date, 12% of the total complaints received by OVIC concern council's inappropriate handling of personal information. Fifteen percent of these complaints relate to councillors directly. Similarly, it was 28% of total complaints in 2023-24 and 29% in the 2022-23 financial years respectively.

Common themes that arise in these complaints include:

- unauthorised access to council systems and misuse of personal information for non-legitimate purposes
- use of council systems and personal information for personal benefit during a council election
- council employees sending council information to their personal email addresses for unknown purposes, including contact information databases and financial/invoice databases
- insufficient steps being taken to protect personal information, including:
    - failure to redact documents before publication or release through FOI
    - inappropriate use of AI tools
    - insufficient training and awareness of information handling practices.

The Privacy Guidance and Dispute Resolution Unit work with organisations who have had a complaint made against them to gain a comprehensive understanding of the factors that led to the complaint. As part of the conciliation process, OVIC may provide guidance to that organisation to implement practices that prevent similar occurrences in the future.

[7] See https://ovic.vic.gov.au/information-security/information-security-resources/protective-data-security-plan-insights/.

Information security

Councils are explicitly excluded from Part 4 of the PDP Act. Despite this, some councils either incur obligations under Part 4 arising from their administration of a body subject to Part 4 or they choose to voluntarily engage with OVIC.

In 2024, 77 of the 79 local Councils submitted a PDSP. These PDSPs do not necessarily reflect the information security management program of all council information and systems. Rather, they may be limited to the regulated organisation that the council administers, such as Committees of Management or Cemetery Trusts. Broadly speaking, councils that submitted a PDSP commonly responded with an average implementation status of *Partial (some)* or *Partial (most)* for each of the Standards. These implementation levels are relatively consistent when compared against whole of Victorian Government reporting.

The total number of incidents reflected across the PDSPs submitted by councils in 2024 was 4,329.[8] The PDSP reporting also indicated that this included 859 incidents that reached a business impact level 2 or higher. Notification of incidents through OVIC's ISINS indicates that reports from local government have continued to steadily rise between the period of January 2022 to June 2024.

Freedom of information

The FOI Act provides transparency and accountability for council decision making by enabling the public to request access to documents created by councils. This transparency requirement helps mitigate fraud and corruption risks. Requests for access to documents under the FOI Act are made to the agency directly. However, where an applicant believes there is a problem with how that agency has handled the processing of their request, or the applicant is unhappy with the agency's ultimate FOI decision about the release of documents, the applicant can make a complaint to OVIC and/or request OVIC review the agency's FOI decision. Through this process, OVIC regularly observes that applicants are seeking to use the FOI process to uncover fraud and corruption. Section 30(1) of the FOI Act outlines a test determining whether disclosure of information or documents would be contrary to the public interest. Where documents reveal misconduct, fraud and corruption, the public interest may weigh in favour of disclosure.

In September 2024, OVIC welcomed the tabling of the Integrity and Oversight Committee's report following its Inquiry into the operation of the Freedom of Information Act 1982.[9] This report recommended whole scale legislative reform to replace Victoria's outdated FOI laws with a modern 'right to information' law. OVIC fully supports this recommendation and considers such reform would make it easier overall for people to access government-held information and would further increase transparency and mean greater oversight of councils and their decision-making processes.

[8] Of the 77 PDSPs, one was received after the cut-off date. This means that these statistics are based on 76 PDSPs.
[9] See https://www.parliament.vic.gov.au/foi-report

Ineffective information security or privacy controls could increase the risk of fraud and corruption.

Ineffective controls increase the potential for risks to manifest, including risks relating to fraud and corruption. There is no legislative requirement for councils to apply any specific information security controls to council information or systems. Even where councils voluntarily accept OVIC's recommendation to implement the VPDSS, the implementation of controls may be somewhat unstructured.

The lack of a legislative requirement under Part 4 also creates confusion across the sector, further compromising efforts to enhance information security. The local government-related privacy complaints received by OVIC largely relate to adverse impacts on the confidentiality, availability or integrity of personal information.

Regulatory schemes must have visibility mechanisms that provide sector insights. OVIC is of the view that changes must be made to reduce the risk of fraud and corruption in local government and the broader VPS. The current reporting arrangements mean reduced visibility for OVIC and increased opportunities for councils or council employees to conceal fraud and corruption involving the misuse of information and systems.

Furthermore, councils are part of a broader information ecosystem spanning across the VPS. Councils hold information that other VPS agencies are obligated to impose stringent information security controls on. Having different information security obligations on the same information in different organisations is benign and makes councils a greater target for fraud, corruption and information security threats. Similar to this, there are information sharing mechanisms between some councils and other VPS agencies. Notwithstanding OVIC's current lack of visibility over the sector, it is more than conceivable that a lack of information security practices increases the risk of compromise of these systems through local government.

The exclusion of councils from Part 4 means there is no obligation for councils to implement consistent information security controls and a lack of oversight and visibility. This increases opportunity for councils or council employees to perpetrate and conceal fraud and corrupt activity. Subjecting councils to Part 4 of the PDP Act would reduce this opportunity by imposing stronger information security obligations on the organisation.

The VPDSS, which apply to all bodies bound by Part 4 of the PDP Act, include standards for personnel as well as systems. These standards require organisations to ensure that personnel in trusted roles have some level of probity checks. Personnel security practices reduce the risk of an organisation hiring an employee that is susceptible to engaging in, or facilitating, fraud and corruption activity.

Existing legislative and regulatory frameworks are not adequate to mitigate the risks of fraud and corruption

Parts 3 and 4 of the PDP Act should work in tandem with each other. Excluding entities from Part 4 means greater risk to compliance with Part 3, since a lack of information security controls means personal information is less secure. This is why the existing legislative framework is not adequate to mitigate the risks of fraud, corruption and broader information incidents.

OVIC recommends the following changes to the PDP Act:

- The establishment of a mandatory information security incident notification scheme
- The removal of exclusions to Part 4 of the PDP Act.

Mandatory information security incident notification scheme

Victoria does not have a mandatory information security incident notification scheme where all VPS organisations are required to notify the oversight body and individuals whose information has been compromised following an incident. This puts Victoria far behind other Australian jurisdictions, including New South Wales, Queensland, Western Australia and the Commonwealth.[10]

Currently in local government, OVIC is only aware of an incident if a privacy complaint is made or if the organisation voluntarily reports it under the ISINS. If councils were subject to a mandatory information security incident notification scheme, all incidents of a certain threshold would be required to be reported to OVIC by the organisation.

According to a 2017 study by the Office of the Australian Information Commissioner, 95% of Australians believe that if a government agency loses their personal information, they should be informed.[11] Notification for individuals empowers them to take time sensitive remedial action to protect their personal information, and in extreme cases, their safety. For example, individuals may move house if subject to domestic violence, change passwords, cancel credit cards, and update identity documents.

Therefore, under a mandatory information security incident notification scheme, OVIC should have powers to require an organisation to notify individuals affected by a breach and in some cases, make a public statement about the incident. A mandatory information security incident notification scheme should apply across the entire VPS, not just local government.

OVIC has undertaken extensive research on how a mandatory incident notification scheme could operate in Victoria and would be pleased to share further details on this issue with the Committee.

All agencies should be subject to Part 4 of the PDP Act

Councils hold a wide range of personal information, and information about their own services, that are in need of protection. This information makes councils targets for threat actors both external and internal to the organisation. The lack of mandatory information security obligations, coupled with threat actors' knowledge of this, makes the target more appealing. Local government is also part of

[10] The Commonwealth and New South Wales have established privacy incident notification schemes. Queensland's scheme will come into effect in July 2026, and Western Australia's recently passed *Privacy and Responsible Information Sharing Act 2024* contains a notifiable information breaches scheme.
[11] Australian Community Attitudes to Privacy Survey 2017 report, https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2017-report#figure16.

the broader VPS information ecosystem. Any deficiencies in a council's information security program can, by extension and integration, potentially adversely impact other VPS organisations.

Subjecting local councils to Part 4 would bring information security practices of those entities under the jurisdiction of OVIC. OVIC would be able to provide more targeted guidance in the implementation and maintenance of best practice information security across all security domains through the VPDSS. Further, the requirement for councils to provide organisation-wide PDSPs would enhance OVIC's visibility over the sector. While OVIC currently receives PDSPs from most councils, many only relate to the information holdings of components that are already subject to Part 4, such as Committees of Management or Cemetery Trusts. However, since most councils are familiar with PDSPs, this expansion would not require councils to start this process from the beginning but rather build on existing knowledge.

Any expansion of Part 4 must also include other organisations currently excluded, such as courts, tribunals, universities and hospitals. Evidence shows that threat actors are increasingly targeting these sectors, with data breaches, cyber-attacks, and ransomware attacks now considered an expectation rather than a mere possibility. For example, OVIC is aware that incidents are occurring in entities such as courts and tribunals. These entities are exempt under section 10 of the PDP Act from the IPPs and VPDSS in relation to their judicial or quasi-judicial functions. Essentially, this places courts and tribunals beyond the oversight of OVIC and renders that sector completely opaque in terms of incidents that are occurring, unless the entity self-reports. Not knowing what kind of incidents are occurring and when they are occurring means harm caused by these incidents cannot be minimised effectively and vulnerable Victorians' information cannot be protected. Furthermore, like local government, these agencies are a part of the VPS information ecosystem. This means information security deficiencies in these agencies increase information security risks in other VPS organisations.

The relationship between OVIC and integrity agencies, such as the Local Government Inspectorate, in managing suspicions or allegations of fraud and corruption related to information security in local government.

As discussed, OVIC has limited visibility and jurisdiction over the information security practices of local government entities. Allegations of information misuse in privacy complaints allow OVIC to assist the responding organisation to implement systems that prevent the kind of misuse identified in the complaint from occurring in future.

OVIC is currently examining a process whereby it can share business intelligence, subject to any applicable secrecy or confidentiality obligations, with other integrity agencies. While the Local Government Inspectorate is a regulator rather than an integrity body, the intention is to include them in this process. Furthermore, referral pathways between OVIC and other integrity agencies already exist. When OVIC receives a complaint or enquiry concerning a matter in another agency's jurisdiction, OVIC will direct the person making the enquiry to that agency.