Office of the Victorian Information Commissioner

7 July 2025

Sarah Connolly MP
Chair, Public Accounts and Estimates Committee
Parliament House
EAST MELBOURNE VIC 3002

By email only: localgovfraudcorruption@parliament.vic.gov.au

Attendance at a public hearing for the Public Accounts and Estimates Committee's Parliamentary Inquiry into fraud and corruption control in local government

Dear Chair

Thank you for the invitation to attend a public hearing for the Public Accounts and Estimates Committee's Inquiry into fraud and corruption control in local government. I accept the invitation and look forward to contributing further to this important inquiry. Please see below the requested written statement preceding my appearance before the Committee.

If OVIC can be of further assistance before my appearance at the public hearing, please contact us through [redacted]

Yours Sincerely

[redacted]

Sean Morrison
Victorian Information Commissioner

Written statement accompanying the Information Commissioner's attendance to the Public Accounts and Estimates Committee's Inquiry into fraud and corruption control in Local Government.

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 as 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 that apply to Victorian Government information and systems should also apply to local government information and systems.

Local councils are excluded from Part 4 of the *Privacy and Data Protection Act 2014* (PDP Act). This means that they are not subject to the obligations arising from Part 4 including the Victorian Protective Data Security Framework and Victorian Protective Data Security Standards (VPDSS). However, local councils are also often appointed as Committees of Management for Crown land reserves and as trustees of Cemetery 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.

In its submission to the Inquiry into fraud and corruption control in local government[1], OVIC made the following recommendations that relate directly to preventing fraud and corruption in local government through enhancing information security.

Recommendation 1: Introduce a 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.

Currently in the local government context, OVIC is only aware of an incident if a privacy complaint is made or if the organisation voluntarily reports. 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.

[1] OVIC. 2025. *Submission to the Inquiry into fraud and corruption control in local government*. https://www.parliament.vic.gov.au/496266/contentassets/b0ffb2869f2245d798e9702c7049cb93/submission-documents/11.-office-of-the-victorian-information-commissioner-no-ltr.pdf

Reporting information security incidents can lead to early detection of fraud or corrupt behaviour within councils. It also enables victims of a data breach to take remedial action to protect their personal information, and in extreme cases, their safety. OVIC has undertaken extensive research on how a mandatory information security incident notification scheme could work in Victoria and would be pleased to share further details on this issue with the Committee.

Recommendation 2: All organisations should be subject to Part 4 of the Privacy and Data Protection Act 2014

As referenced earlier, councils hold a wide range of personal information, and information about their own services, that requires 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 gap, makes the target more appealing. Local government is part of 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 of the PDP Act would bring the 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. OVIC is aware that councils have varying resourcing challenges and varying information security maturity levels. Councils currently have information security reporting arrangements where they administer an entity such as a Committee of Management. Councils also have experience reporting to OVIC due to obligations arising with administration of these, and similar entities. OVIC is of the view that, by leveraging existing experience and reporting mechanisms, making councils subject to Part 4 of the PDP Act would be a low impost policy solution to remedy the risk of fraud and corruption arising from poor information security practices.

Shared services and IT system centralisation

OVIC notes the Committee's interest in local government IT system centralisation in the first round of public hearings. Most importantly, without a proposed model to review, it is difficult to conduct an assessment of this model. This is because the assessment is influenced by many factors including:

- the specific risks that the model seeks to address
- which services and datasets are selected for centralisation
- the technical and physical components of the model
- the varying information assets, management and security maturity across different councils
- governance arrangements including proposed support models for the system.

The Victorian Auditor-General's Office conducted an audit on Shared Services in Local Government in 2014. The report found that while there were financial benefits to shared services in local government, there was inadequate monitoring and evaluation to clearly observe or substantiate these

expected benefits. The report also notes that when identifying the main reasons councils pursued shared service initiatives, none of the 6 audited councils identified improving integrity as a reason.

Further exploration of centralisation across councils must be prefaced by a comprehensive risk assessment. This process would ensure that risks are clearly identified, their root causes understood, and their potential impacts evaluated. This would provide a clear basis for the design of targeted controls and ensure that any proposed solution is both risk-informed, evidence-based and proportionate to the level of risk-exposure. A centralisation proposal developed without this initial assessment may miss key threats, apply ineffective controls or be unable to realise its intended benefits. OVIC would be pleased to speak further about these issues at the hearing.