

VAGO

Victorian Auditor-General's Office



Security and Privacy of Surveillance Technologies in Public Places

September 2018

Independent assurance report to Parliament
2018–19: 9



Security and Privacy of Surveillance Technologies in Public Places

Independent assurance report to Parliament

Ordered to be published

VICTORIAN GOVERNMENT PRINTER

September 2018

PP no 439, Session 2014–18

This report is printed on Monza Recycled paper. Monza Recycled is certified Carbon Neutral by The Carbon Reduction Institute (CRI) in accordance with the global Greenhouse Gas Protocol and ISO 14040 framework. The Lifecycle Analysis for Monza Recycled is cradle to grave including Scopes 1, 2 and 3. It has FSC Mix Certification combined with 99% recycled content.

ISBN 978 1 925678 32 1



The Hon Bruce Atkinson MLC
President
Legislative Council
Parliament House
Melbourne

The Hon Colin Brooks MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of section 16AB of the *Audit Act 1994*, I transmit my report *Security and Privacy of Surveillance Technologies in Public Places*.

Yours faithfully

A handwritten signature in black ink, appearing to read "Andrew Greaves", is written over a faint, light blue circular stamp. The signature is fluid and cursive.

Andrew Greaves
Auditor-General

19 September 2018

Contents

Audit overview	7
Conclusion	8
Findings.....	9
Recommendations.....	10
Responses to recommendations	11
1 Audit context	13
1.1 Surveillance in public places	13
1.2 Privacy legislation	14
1.3 Regulation and guidance	16
1.4 Council surveillance	19
1.5 Why this audit is important	21
1.6 What this audit examined and how	22
1.7 Report structure	22
2 Management and oversight	23
2.1 Conclusion	23
2.2 Council policies and procedures	24
2.3 Approval of surveillance devices	27
2.4 Managing council CCTV systems	28
2.5 Arrangements with Victoria Police	33
2.6 Improving oversight of public safety CCTV systems	35
2.7 Governance, assurance and accountability	37
3 Privacy and data security	41
3.1 Conclusion	41
3.2 Collection, information and signage.....	42
3.3 Data security.....	45
3.4 Use, disclosure and access.....	51
3.5 Inappropriate use	54
3.6 Complaint handling	55
Appendix A. <i>Audit Act 1994</i> section 16—submissions and comments	57
Appendix B. Arrangements with Victoria Police for public safety CCTV systems.....	75
Appendix C. Site pictures of CCTV signage and equipment.....	81
Appendix D. Detailed findings on use, disclosure and access	83

Acronyms

CCTV	closed-circuit television
CPDP	Commissioner for Privacy and Data Protection
ICT	information and communications technology
MoU	memorandum of understanding
OVIC	Office of the Victorian Information Commissioner
PDPA	<i>Privacy and Data Protection Act 2014</i>
PROV	Public Record Office Victoria
VAGO	Victorian Auditor-General's Office
VPDSF	Victorian Protective Data Security Framework

Audit overview

Across the public and private sectors, organisations use a range of technologies to observe or monitor individuals or groups, such as closed-circuit television (CCTV) surveillance systems. Some Victorian local councils, use CCTV for public safety and protecting council staff and assets.

Councils' CCTV surveillance systems fall into two main categories:

- Public safety CCTV systems—councils install these systems to discourage and detect antisocial and criminal behaviour in public places. Victoria Police has direct access to monitor and review footage from these systems. The initial purchase costs are usually funded by grants from the state or Commonwealth governments, with councils funding ongoing maintenance and replacement costs.
- Corporate CCTV systems—councils fund the installation of these systems and use them to monitor facilities that include public spaces, such as council offices, pools, libraries, performing arts centres and waste management facilities. These systems are typically managed onsite by council employees or contractors.

Surveillance systems in public places impact on the privacy of individuals, so it is important that councils can demonstrate to their communities that they are managing these systems well and in compliance with privacy requirements. If councils cannot demonstrate this, they risk losing public confidence.

The *Privacy and Data Protection Act 2014* (PDPA) sets out Information Privacy Principles that apply when public sector agencies, including councils, collect personal information that enables individuals to be identified, such as the images captured by CCTV systems. The Office of the Victorian Information Commissioner (OVIC), formerly the Commissioner for Privacy and Data Protection (CPDP), has a key role in implementing and supporting compliance with PDPA. Before OVIC was established, CPDP issued *Guidelines to surveillance and privacy in the Victorian public sector* in May 2017. We used this and other comprehensive guidance material on the use of CCTV in public places as criteria for our audit.

Local councils are using advances in surveillance technology legitimately to collect information about people's daily activities. In parallel, they need to fulfil their responsibility to respect individuals' right to privacy, by ensuring that the information from their surveillance devices is securely collected, stored and transmitted. The absence of community objections to surveillance in public places does not diminish this responsibility, and councils need to demonstrate organisational leadership through robust policies, strong management and controls, and effective oversight.

In this audit, we assessed whether councils keep secure the information they collect from their CCTV systems and whether they protect the privacy of individuals. Specifically, we assessed the management and use of surveillance devices in public places by five councils to see whether they adhere to relevant privacy laws and appropriate use policies, and whether they protect the information they collect from unauthorised disclosure.

The councils we audited were the City of Melbourne (Melbourne), Whitehorse City Council (Whitehorse), Hume City Council (Hume), East Gippsland Shire Council (East Gippsland) and Horsham Rural City Council (Horsham). Between them, these councils have more than 1 100 CCTV cameras and they are increasing their use of surveillance devices.

Victoria Police was not included in our audit scope. However, as it is the key user of public safety CCTV systems, we examined council-owned CCTV systems in police stations and spoke to police officers involved in using these systems.

Conclusion

The councils we examined in this audit could not demonstrate that they are consistently meeting their commitments to the community to ensure the protection of private information collected through CCTV systems.

The audited councils advised that they have never found an incident of inappropriate use of surveillance systems or footage, and OVIC advised that it has never received a complaint about such use. However, given the weaknesses that we identified in security and access controls, and the lack of review of how CCTV systems are being used, the absence of evidence of inappropriate use of council CCTV doesn't provide strong assurance that no such incidents have occurred.

Gaps in councils' CCTV system signage, management and oversight mean the councils are unable to demonstrate that their CCTV activities adhere to the requirements of PDPA, including appropriate use and sufficient protection of the information collected from unauthorised disclosure. Where councils do undertake monitoring and assurance activities, they are largely restricted to public safety CCTV systems. This means that councils are not adequately scrutinising the operation and use of most of their CCTV systems.

Councils can improve the security of the personal information they gather through their CCTV systems to better protect the privacy of individuals.

Improving physical security and access controls will better enable councils to ensure that access to and use of these systems is appropriate and that the information collected from their surveillance activities in public places is protected from unauthorised disclosure.

Management and oversight

Except for Horsham, all the audited councils have a policy to guide their management of CCTV systems. However, in most cases, these policies focus on public safety CCTV systems, and councils do not have robust, documented operating procedures to support the sound management of their corporate CCTV systems.

Only East Gippsland could demonstrate that decisions to install new CCTV cameras in public places are informed by consideration of privacy impacts, and there was also only limited evidence of community consultation about new cameras at any of the councils.

Apart from Melbourne, none of the councils have adequately used their agreements with Victoria Police to ensure proper oversight of and accountability for the use of public safety CCTV systems. The agreements between police and councils require the councils to establish a steering committee and an audit committee to oversee and review these systems. These oversight committees varied in their effectiveness—typically, they meet rarely and when they do they focus on operational issues such as camera location and functionality rather than privacy and data security.

Corporate CCTV systems arguably pose greater privacy and data security risks than public safety systems because they are dispersed across many locations and are subject to local operating practices that are not guided by robust procedures. Only Melbourne and East Gippsland had sufficient senior management involvement in the use of corporate CCTV systems, and none of the audited councils reported regularly on these systems.

In addition, none of the councils had formal committees or assurance processes to oversee the management and use of their corporate CCTV systems. As a result, senior management and councillors lack adequate assurance that their CCTV systems are managed appropriately.

Where formal monitoring and assurance activities do occur, they are largely restricted to public safety CCTV systems which typically make up 20 per cent or less of council CCTV systems. Councils do not routinely scrutinise the operation and use of their corporate CCTV systems.

Regular reporting on key metrics for all corporate CCTV systems—such as the number of times council staff reviewed CCTV footage, saved or copied CCTV footage, and provided copies of footage to external parties—would make senior management aware of these surveillance activities, support a culture of appropriate use, and promote more active management.

Melbourne and East Gippsland are the only councils to provide regular public reporting on the use and management of their CCTV systems. However, even these councils report only on public safety CCTV systems rather than all their CCTV systems.

Privacy and data security

It is positive that the audited councils have not found any instances of inappropriate use of surveillance systems or footage. We found that councils have good awareness of the privacy issues associated with the use of CCTV systems.

However, all five councils can improve the security of the personal information they gather through their CCTV systems to better protect the privacy of individuals. Key areas to address include improving physical security and access controls for corporate CCTV systems and regularly assessing whether those controls are working.

All of the audited councils use generic user logins for corporate CCTV systems, and some do not use system activity logs to track usage. These practices increase the risk of inappropriate use occurring and going undetected. There are similar issues with public safety CCTV systems.

Improving physical security and access controls will better enable the councils to protect information collected from council surveillance activity from unauthorised disclosure.

In addition, we found at least one site at each council where they operate CCTV in public spaces without adequate public signage.

Recommendations

We recommend that the City of Melbourne, Whitehorse City Council, Hume City Council, East Gippsland Shire Council and Horsham Rural City Council:

1. review and update their CCTV policies to address the requirements of the *Privacy and Data Protection Act 2014* (see Section 2.2)
2. assess all CCTV systems installed prior to the approval of a CCTV policy to ensure they comply with the policy (see Section 2.2)
3. assess the privacy impacts of proposals to install new or additional CCTV surveillance devices in public places (see Section 2.3)
4. develop site-specific operating procedures for their corporate CCTV systems to reflect the requirements of the *Privacy and Data Protection Act 2014* and their policies (see Section 2.2)
5. allocate responsibility for overseeing the operation of CCTV systems to an appropriate senior manager and implement regular reporting on key aspects of CCTV system use (see Section 2.4)
6. include a periodic audit of CCTV system use and data security in their forward internal audit programs (see Section 2.7)
7. review and update the content and position of all signage in locations with corporate CCTV systems to reflect better practice (see Section 3.2)

8. review and address access control and data security weaknesses for corporate CCTV systems (see Section 3.3)
9. ensure regular audits and evaluations of public safety CCTV systems and hold the oversight committees for these systems to account for meeting their responsibilities under agreements with Victoria Police (see Sections 2.5 and 2.6).

We recommend that the Horsham Rural City Council:

10. establish and implement a policy to cover all council CCTV systems (see Section 2.2).

We recommend that the Whitehorse City Council:

11. establish an agreement with Victoria Police for the public safety CCTV system at the Box Hill mall and laneways (see Section 2.5).

Responses to recommendations

We have consulted with the Melbourne, Whitehorse, Hume, East Gippsland and Horsham councils, and we considered their views when reaching our audit conclusions. As required by section 16(3) of the *Audit Act 1994*, we gave a draft copy of this report to those agencies and asked for their submissions or comments. We also provided a copy of the report to the Department of Premier and Cabinet.

The following is a summary of those responses. The full responses are included in Appendix A.

All councils accepted the recommendations.

Melbourne, East Gippsland and Horsham provided action plans noting their intended actions and timelines for addressing each recommendation.

Whitehorse and Hume did not provide an action plan addressing each specific recommendation but provided information on how they will approach addressing the audit recommendations and the timelines for this work.

1

Audit context

1.1 Surveillance in public places

Recent advances have made surveillance technology—ranging from familiar tools such as CCTV to more sophisticated technologies such as drones and facial recognition, a form of biometric technology—more readily available, affordable and sophisticated. CCTV cameras, the focus of this audit, are increasingly used in public spaces like streets, shopping centres, shops, banks, public transport and car parks as a crime prevention measure and as a tool to detect and identify offenders.

More recently, the Internet-of-Things (the expansion of the internet from something that most people only use through their personal computer or mobile device to something that is connected to everyday physical objects such as home security cameras, microwave ovens, and refrigerators) has also been identified as a potential way to undertake surveillance activities.

Research has shown that there is community support for the use of some types of surveillance devices in public places, however, this support is not universal. Community members may be concerned about the loss of privacy in public places as these devices capture personal information and can monitor the movements of individuals. There is also the risk that information collected by these devices may be misused.

What is surveillance?

A May 2010 report from the Victorian Law Reform Commission, *Surveillance in Public Places*, defines surveillance as the deliberate or purposeful observation or monitoring of a person, object or place.

Under the *Surveillance Devices Act 1999* surveillance devices include data surveillance devices, listening devices, optical surveillance devices and tracking devices. An optical surveillance device is one that can visually record or observe an activity.

Except for authorised law enforcement activities, the *Surveillance Devices Act 1999* prohibits a person from installing, using or maintaining optical surveillance devices to observe or record other people in private without their express or implied consent. The *Surveillance Devices Act 1999* excludes activity carried on outside a building or in a place where people cannot have a reasonable expectation of privacy from the definition of private activity.

CCTV surveillance devices managed by public sector agencies and councils are largely visible in public places where the *Surveillance Devices Act 1999* allows the use of optical surveillance devices to record people without consent. There should be signage in the areas under surveillance informing people that CCTV is in use.

Public place

The *Summary Offences Act 1966* defines a ‘public place’ as including:

- any public highway, road, street, bridge, footway, footpath, court, alley, passage or thoroughfare even if it is on private property
- any park, garden reserve or other place of public recreation or resort
- any railway station, platform or carriage
- any public vehicle available for hire
- any government school
- any market.

For the purposes of this audit, our definition of public places also included places owned, managed or controlled by the audited councils to which the public have access, such as council offices and other buildings and locations, including sporting, leisure and recreation facilities.

1.2 Privacy legislation

Within the definition of ‘personal information’, PDPA also includes information that is recorded in any form about an individual whose identity is apparent, or can be reasonably ascertained, from the information.

PDPA is the primary legislation regulating privacy and data collection in the Victorian public sector. It requires agencies to collect and handle ‘personal information’ responsibly. It provides remedies for interference with the information privacy of individuals and establishes a protective data security regime for the public sector. PDPA includes some specific requirements for agencies:

- Information privacy—information privacy is a recognised human right. PDPA specifies 10 Information Privacy Principles to govern how agencies, including local councils, and public sector contractors collect, use and handle personal information. The core objective of these principles is to balance public interest in the free flow of information with protecting the privacy of personal information.
- Data security—PDPA requires the creation of a Victorian Protective Data Security Framework (VPDSF) covering data security risk management for all Victorian public sector information, including personal information. Protective data security standards can be issued under PDPA to support the framework, and PDPA also imposes compliance obligations on public sector agencies.

The Information Privacy Principles have been in place since 2000, and compliance is mandatory for local government councils and all public sector agencies. Figure 1A summarises the principles most relevant to councils' surveillance activities.

Figure 1A
Information Privacy Principles relevant to councils' surveillance activities

Principle	Key requirements
1 Collection	<p>The organisation must:</p> <ul style="list-style-type: none"> not collect personal information unless it is necessary for one or more of its functions or activities collect information by lawful and fair means and not in an unreasonably intrusive way take reasonable steps to ensure that individuals are aware of: <ul style="list-style-type: none"> the identity of the organisation the purpose for which the information is collected the fact that the individual is able to access collected information other organisations to whom it usually discloses the information.
2 Use and disclosure	<p>The organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection unless certain circumstances apply. If an organisation uses or discloses personal information for law enforcement purposes, it must make a written note of the use or disclosure.</p>
3 Data quality	<p>An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.</p>
4 Data security	<p>An organisation must take reasonable steps to:</p> <ul style="list-style-type: none"> protect the personal information from misuse and loss and from unauthorised access, modification or disclosure destroy or permanently de-identify personal information if it is no longer needed for any purpose.
5 Openness	<p>The organisation must:</p> <ul style="list-style-type: none"> document clearly expressed policies on its management of personal information and make this available to anyone who asks for it take reasonable steps to let people who request it know what sorts of information it holds, for what purposes and how it collects, holds, uses and discloses that information.
6 Access and correction	<p>If an organisation holds personal information about an individual, it must provide the individual with access to the information on request, unless certain circumstances apply including where providing access would have an unreasonable impact on the privacy of other individuals, be unlawful or prejudice law enforcement activities.</p>

Source: VAGO based on PDPA.

Information Privacy Principle 4 deals with data security. OVIC has advised councils that they can best meet this requirement by applying relevant content from the VPDSF and related standards.

OVIC's predecessor, CPDP, examined the websites of all 79 Victorian councils in 2016 to assess the level of information disclosed on CCTV use and its privacy implications. It found that:

- 82 per cent of councils made a general privacy policy available to the public on their websites, however, only two policies explicitly mentioned the use of CCTV
- only 19 per cent of councils provided a standalone CCTV policy
- 84 per cent of councils did not adequately explain how they handle the personal information they gather through CCTV
- only 30 per cent of councils with a privacy policy had easily accessible contact details for privacy-related matters
- just 7 per cent of councils with a privacy policy explained how citizens could access, modify or delete their personal information.

1.3 Regulation and guidance

OVIC was created in September 2017 when CPDP merged with the Freedom of Information Commissioner. OVIC administers PDPA and has specific functions to support and monitor information privacy and data security.

Authoritative guidance available to councils on the use and oversight of surveillance technology to protect privacy and data security includes:

- *Guide to Developing CCTV for Public Safety in Victoria*, issued by the former Department of Justice in August 2011 and updated by the Department of Justice and Regulation in June 2018
- *Closed Circuit Television in Public Places—Guidelines*, issued by the Victorian Ombudsman in November 2012
- *Guidelines to surveillance and privacy in the Victorian public sector*, issued by CPDP in May 2017.

Figure 1B summarises the key features and principles of this guidance. We used this guidance and these principles as our criteria when assessing council performance in this audit.

Figure 1B

Key guidance for councils on surveillance technologies in public places

Component	Key principles and guidance
Management and oversight	
Policies and procedures	<p>Councils should have clear policies to govern the installation, use and oversight of all surveillance technologies. The policies should set minimum expectations for decisions about installing surveillance devices, privacy considerations, the collection, management and use of information, physical and data security, access, disclosure, storage, retention and disposal of surveillance information, governance and oversight arrangements, monitoring, evaluation and accountability.</p> <p>A comprehensive policy needs to be supported by operating and procedure manuals or instructions to guide the day-to-day management and use of surveillance systems. These can take many forms but need to go beyond system technical manuals.</p>
Approval of surveillance devices	<p>Councils should have a clear framework and process for assessing and deciding whether to install surveillance devices in public places. Essential considerations include:</p> <ul style="list-style-type: none"> • confirming that proposed surveillance is for a legitimate council objective or function and consistent with applicable laws • clarity about the intended purpose of surveillance • alternatives to surveillance • consultation with affected communities including residents, traders and business owners • consultation with authoritative stakeholders and regulators such as OVIC, Victoria Police and the Public Record Office Victoria (PROV) • impacts on privacy and whether proposed surveillance is a proportionate response to the issue or risk to be addressed • how the surveillance information and data will be kept secure and protected from inappropriate use or disclosure • costs and benefits and how councils will assess the effectiveness of their surveillance activities.
Resourcing and management arrangements	<p>Councils should be clear about who is responsible for the management and oversight of surveillance activities. Day-to-day management of separate surveillance systems can be devolved to local staff, but there should be a senior manager responsible for overseeing this activity.</p> <p>Staff involved in using and managing surveillance systems should be properly trained.</p> <p>There should be regular reporting on key aspects of surveillance activities.</p> <p>Councils should understand and consider the whole-of-life costs associated with installing, supporting, maintaining, upgrading, replacing and managing surveillance systems.</p>
Agreements with Victoria Police	<p>Councils need a formal agreement with Victoria Police if they intend to share or disclose surveillance information, to provide clarity on:</p> <ul style="list-style-type: none"> • obligations and responsibilities of the parties • ownership of the surveillance system and the data it generates • oversight and review mechanisms, including how the council will be assured that Victoria Police is using and managing the information provided appropriately.
Governance, assurance and accountability	<p>Councils should establish review and audit mechanisms to examine their surveillance activities. Audits, reviews and evaluations should be independent of program management, and the results reported to the community.</p> <p>Councils should consider assigning responsibility for oversight of surveillance activities to a separate specialist, or existing council steering or audit committee or governance group. This committee or group should regularly scrutinise surveillance activities against their intended purposes, the law, and council policies and procedures. Members of any specialist committee can include people with relevant expertise, community representatives and key users such as Victoria Police.</p>

Figure 1B

Key guidance for councils on surveillance technologies in public places—*continued*

Component	Key principles and guidance
Privacy and data security	
Collection, information and signage (Information Privacy Principle 1)	<p>Councils should:</p> <ul style="list-style-type: none"> • take reasonable steps to make people aware that surveillance devices are in use in a public place and how they can obtain information about their use • make their policies and other information on the use of surveillance systems easily accessible to the community.
Data Security (Information Privacy Principle 4)	<p>Councils should take reasonable steps to protect the personal information they hold against misuse, loss, unauthorised access, modification or disclosure.</p> <p>Ensuring data security involves:</p> <ul style="list-style-type: none"> • physical security over surveillance devices and equipment • security controls on the information and communications technology (ICT) used in the devices and equipment • limiting access to surveillance footage and records to individual officers and contractors with a need to know • taking steps to detect and deter security breaches.
Use, access and disclosure (Information Privacy Principle 2)	<p>A fundamental principle of privacy law is that individuals have a right to seek access to the personal information an organisation holds about them. Councils need to make information freely available to the public about how to request access to surveillance information and consider how they will deal with requests for access. Councils should apply their freedom of information process to such requests.</p> <p>Surveillance footage and records should generally only be used and disclosed to a third party in accordance with the primary purpose of collection. If considering disclosing surveillance footage to an individual or others, councils should examine whether doing so would infringe on the privacy of other individuals.</p> <p>Councils should have a written procedure to address breaches of surveillance policies and procedures and the misuse of surveillance systems and footage. Contracts or agreements with external parties provided access to surveillance equipment and footage should address inappropriate use.</p> <p>Councils should comply with requirements for the management of public records and delete information gathered through surveillance activities once it is no longer required.</p>
Complaint handling	<p>Councils should inform their communities of their right to make a complaint about the use of council surveillance technologies and consider any such complaints under their established complaints handling process.</p>

Source: VAGO based on the former Department of Justice, *Guide to Developing CCTV for Public Safety in Victoria*, 2011; Victorian Ombudsman, *Closed Circuit Television in Public Places—Guidelines*, 2012; CPDP, *Guidelines to surveillance and privacy in the Victorian public sector*, 2017.

1.4 Council surveillance

Local councils are significant users of CCTV surveillance systems in the Victorian public sector. Councils place CCTV cameras in and around customer service areas, council buildings and facilities, recreation and activity centres and landmark buildings, and may also use them during major events.

Many councils have used grants from the Commonwealth and state governments to install public safety CCTV systems for use by Victoria Police in public areas known to have high rates of antisocial behaviour or crime. Victoria Police's stated policy position is that it will not directly access council CCTV information without having a formal memorandum of understanding (MoU) in place to govern the protocols around the transfer of information.

Information Privacy Principle 1 states that public bodies must not collect personal information unless it is necessary for one or more of their functions or activities. Councils can satisfy this requirement when using surveillance devices by relying on the *Local Government Act 1989* which specifies:

- that improving the overall quality of life of people in the local community is an objective for local councils
- that councils' functions may relate to the peace, order and good government of the municipal district.

The councils we examined are increasing, rather than decreasing, their use of surveillance devices, with some using or considering the use of drones and body-worn cameras for particular purposes. In contrast, some other councils have decided not to use CCTV systems, citing concerns about their effectiveness and the ongoing costs of maintenance, upgrade and replacement.

There is no statewide register of CCTV cameras managed by councils or other public sector bodies. Figure 1C shows that the five councils examined in this audit had more than 1 100 cameras. Councils fund the installation of corporate CCTV systems and the ongoing operation, maintenance and replacement costs for both public safety and corporate CCTV systems.

Figure 1C
Number of CCTV cameras at each of the audited councils

Council	Public safety CCTV cameras	Corporate CCTV cameras	Total CCTV cameras	Cameras per 10 000 residents
Melbourne	72 ^(a)	298	370	27.3
Whitehorse	47	203	250	14.9
Hume	21	297	318	15.9
East Gippsland	22	124	146	32.9
Horsham	31	76	107	53.8
Total	193	998	1 191	

(a) Melbourne expects to have 155 cameras in place through its Safe City Camera Program in the central business district by 31 December 2018.

Source: VAGO based on information from the five councils. Population data sourced from *Victoria in Future 2016: Population and Household Projections to 2031*.

Access and monitoring

Victoria Police has direct access to monitor and review footage from public safety CCTV systems based on operational needs. Councils do not typically have direct access to the footage from these systems. The exception to this is Melbourne, where the council actively monitors the public safety CCTV cameras within its Safe City Camera Program, 24 hours a day, seven days a week. Victoria Police also receives direct transmission from these cameras but needs to contact the council's control room if it wants to review or obtain copies of footage.

Melbourne's public safety CCTV system footage is live streamed to Victoria Police operations centres, police stations within the Melbourne East division and other police stations as specified in the MoU between Melbourne and Victoria Police. A communications link can also be established between Melbourne and the Melbourne Events Operations Centre.

Camera types and locations

The type of CCTV camera used impacts on the risk of privacy breaches and inappropriate use. Pan-tilt-zoom cameras can be used to zoom in on individuals, so they pose higher risks to individuals' privacy and appropriate use. While most public safety CCTV cameras are pan-tilt-zoom enabled, the majority of corporate cameras are not.

Figure 1D provides an overview of the CCTV systems at each council.

Figure 1D**Overview of CCTV systems at the audited councils**

Council	Public safety CCTV systems	Corporate CCTV systems
Melbourne	Covers the Melbourne central business district and surrounds (operational since 1997).	More than 25 including: <ul style="list-style-type: none"> libraries pools council offices tourist attractions managed by council a child care centre.
Whitehorse	Three locations: <ul style="list-style-type: none"> Box Hill mall and laneways (operational since 2011) Box Hill Gardens (operational since 2014) Britannia Mall, Mitcham (operational since 2014). 	More than 15 including: <ul style="list-style-type: none"> libraries council offices pools.
Hume	Sunbury Town Centre (operational since 2013)	More than 15 including <ul style="list-style-type: none"> libraries council offices pools.
East Gippsland	Two locations: <ul style="list-style-type: none"> Bairnsdale (operational since 2014) Lakes Entrance (operational since 2014) 	Around 20 including: <ul style="list-style-type: none"> libraries pools landfills visitor centres council offices. <p>East Gippsland also owns one drone.</p>
Horsham	Horsham Town Centre (operational since 2012)	More than 10 including: <ul style="list-style-type: none"> a performing arts centre and gallery parks landfills a livestock exchange.

Source: VAGO based on information from the audited councils.

1.5 Why this audit is important

The increasing use of surveillance technology by local councils and the potential loss of privacy and misuse of collected information mean that an audit on councils' management of surveillance operations, including processes for sharing information with Victoria Police, is timely.

While there is anecdotal evidence of growing community and media interest in the use of surveillance technologies by government and private entities, there is little hard data demonstrating significant community concern about the privacy and security of the information gathered by the public sector using this technology.

Privacy-related complaints and breaches disclosed to OVIC are growing but numbered fewer than 100 in 2016–17. OVIC’s advice is that none of these privacy complaints or breaches related to the management or use of personal information recorded using CCTV or other surveillance technology by Victorian local government agencies.

There is evidence of increasing use of CCTV by councils and of police requests to access footage collected by councils. This increases the risks to the security of the information gathered and of information privacy breaches. Without formalised policies and procedures to govern the recording, monitoring, transfer and disposal of CCTV footage, the likelihood of these risks eventuating increases.

1.6 What this audit examined and how

This audit examined whether information collected by councils’ CCTV surveillance activities in public places is secure and whether the privacy of individuals is protected. The audit assessed whether:

- the use of council surveillance devices in public places adheres to relevant privacy laws and appropriate use policies
- the information collected from councils’ surveillance activities in public places is protected from unauthorised disclosure.

We audited five councils (three metropolitan and two regional or rural) to provide comparability and contrast. We examined relevant documentation and spoke with council staff and contractors. We visited a wide range of sites where councils have installed corporate CCTV systems, and four Victoria Police stations with public safety CCTV systems.

We conducted our audit in accordance with section 15 of the *Audit Act 1994* and ASAE 3500 *Performance Engagements*. We complied with the independence and other relevant ethical requirements related to assurance engagements. The cost of this audit was \$520 000.

1.7 Report structure

The remainder of this report is structured as follows:

- Part 2 examines councils’ management and oversight of surveillance in public places
- Part 3 examines the privacy and data security of council surveillance activities.

2

Management and oversight

Local councils should be able to demonstrate to their communities that they are managing surveillance systems in public places well. They can achieve this by establishing and implementing robust policies, procedures, management and oversight frameworks and practices.

This part of the report focuses on whether the audited councils can demonstrate this. We examined council policies and procedures, approval of surveillance devices, resourcing, management, governance, assurance and accountability processes and arrangements with Victoria Police.

2.1 Conclusion

All the councils examined, except for Horsham, have a policy to guide their management of CCTV surveillance systems. However, in most cases these policies focus on public safety CCTV systems, and councils do not have robust, documented operating procedures for managing their corporate CCTV systems.

Only East Gippsland could demonstrate that decisions to install new CCTV cameras in public places considered privacy impacts, and there was also only limited evidence of community consultation as part of such decisions at any council.

Apart from Melbourne, none of the councils have adequately used their agreements with Victoria Police to ensure proper oversight and accountability for the use of public safety CCTV systems. The oversight committees for these systems varied in their effectiveness—they typically meet rarely, and do not focus on privacy and data security.

Corporate CCTV systems arguably pose greater privacy and data security risks than public safety CCTV systems, as they are dispersed across many locations and are subject to local operating practices that are typically not guided by robust procedures. Other than at Melbourne and East Gippsland, there was little, if any, senior management oversight of the use of corporate CCTV systems, and none of the councils reported regularly on these systems.

In addition, none of the councils had formal oversight committees or assurance processes to regularly test the appropriate management and use of their corporate CCTV systems. As a result, senior management and councillors lack adequate assurance that their CCTV systems are managed appropriately. Better reporting on the use of corporate CCTV systems would promote more active management and support a culture of appropriate use.

2.2 Council policies and procedures

Councils should have clear policies to govern the installation, use and oversight of surveillance technologies. These policies should cover all CCTV systems and be supported by robust procedure documents.

Policies and procedures for surveillance in public places should cover:

- relevant legislation and privacy principles
- allowable purposes and approval processes for surveillance systems
- what information is to be collected and how and where it can be used and stored
- responsibility for managing and monitoring surveillance activities
- processes for ensuring the security of information collected
- training for staff involved in surveillance activities and systems
- who can access the information, including processes and controls for sharing information with external parties
- how long surveillance information will be retained before disposal
- assurance mechanisms to assess compliance with the law and approved policies and procedures
- the provision of general and accountability information to the public
- dealing with complaints, inappropriate use and privacy breaches.

Policies

All the councils, except for Horsham, had a CCTV systems policy to guide their management and use of CCTV systems. These policies should have been approved before the councils commenced using surveillance devices—however, all councils fell short in this area because they had been operating corporate CCTV systems for years without approved policies. This creates the risk of inconsistent or noncompliant approaches to CCTV installation, management and use.

The timeliness and scope of CCTV policies varies across councils:

- Melbourne established separate policy documents for its public safety and corporate CCTV systems, in 2011 and 2015 respectively. The public safety system began operating in 1997, and many corporate CCTV systems were in place before 2015.
- Whitehorse’s policy covering all of its CCTV systems was approved in 2014 and is currently under review. One of its public safety CCTV systems began operating in 2011.

- Hume’s policy for CCTV systems was not approved until November 2017 despite both its public safety CCTV system and many of the corporate CCTV systems operating before then. The council advised that it intends to carry out further work to implement the policy, including training, compliance checking and regular policy reviews to reflect the lessons learned.
- East Gippsland’s policy was developed for public safety CCTV systems and approved in 2014. This council approved a separate policy for drones in May 2017 and intends to develop a separate policy for corporate CCTV systems. Many of its corporate CCTV systems have been in place since before 2014.
- Horsham does not have a policy despite drafting one for its public safety CCTV system in 2015, three years after it began operating. The council is currently developing a policy.

Figure 2A shows our assessment of councils’ policies, including against the requirements and guidance in Figures 1A and 1B.

Figure 2A
Councils’ policies on CCTV surveillance

Criteria	Melbourne		Whitehorse	Hume	East Gippsland	Horsham
	Public safety CCTV	Corporate CCTV				
Surveillance/CCTV policy first approved	2011	2015	2014	2017	2014	X
Policy covers both public safety and corporate CCTV	✓		✓	✓	Partly ^(a)	X
Policy addresses key elements in guidance:						
• purpose and objectives of CCTV surveillance	✓	✓	✓	✓	✓	X
• CCTV approval process	✓	✓	✓	X	✓	X
• privacy considerations	✓	✓	✓	✓	✓	X
• signage	✓	✓	✓	✓	✓	X
• oversight arrangements	✓	X	✓	✓	✓	X
• reference to council IT policies	X	✓	✓	X	X	X
• training	X	X	✓	✓	X	X
• inappropriate use	✓	X	✓	✓	X	X
• assurance and review mechanisms	✓	X	✓	X	✓	X
• evaluation of effectiveness	✓	X	✓	X	✓	X
• records management	✓	X	✓	✓	✓	X

(a) East Gippsland developed a policy for its public safety CCTV system and applies some requirements to corporate CCTV activities.

Source: VAGO based on assessment of council information.

The most common gaps in councils' CCTV policies related to:

- referencing organisational policies on information technology and security—this was surprising given that CCTV systems clearly involve the collection and storage of information and data using electronic equipment
- training requirements for staff and contractors involved in using CCTV systems
- assurance, review and evaluation processes.

Procedures

The CCTV policy needs to be supported by comprehensive operating and procedure manuals or instructions to guide the day-to-day management and use of surveillance systems. These can take many forms but need to go beyond the technical manuals provided by surveillance technology suppliers. Figure 2B shows our assessment of the CCTV system operating and procedure manuals at the five councils.

Figure 2B
Councils' operating and procedure manuals for CCTV surveillance

Council	Public safety CCTV systems		Corporate CCTV systems	
	Assessment	Comments	Assessment	Comments
Melbourne	✓	Melbourne has a very comprehensive procedures manual for the Safe City Camera Program public safety CCTV system.	✗	Melbourne has a procedure document that applies to the management of all corporate CCTV systems. However, the information in this document is very high level. We found little evidence of detailed operating instructions at the sample sites we visited.
Whitehorse	Partly met	Whitehorse has detailed technical manuals for its public safety CCTV system. It has a short operating manual for only one of its three sites.	✗	Whitehorse could not demonstrate that it had met the commitment in its CCTV policy to develop specific operating manuals for each corporate CCTV system. It provided detailed technical manuals for a few systems but not site-specific operating manuals for use by relevant staff.
Hume	✓	Hume has a detailed technical manual and user guide for the public safety CCTV system located in the Sunbury Town Centre.	Partly met	Hume introduced an organisation-wide standard operating procedure document in November 2017 that applies to the management of all corporate CCTV systems. The information in this document is comprehensive. There are also detailed technical manuals for a few systems but not site-specific operating manuals for use by relevant staff.

Figure 2B

Councils' operating and procedure manuals for CCTV surveillance—*continued*

Council	Public safety CCTV systems		Corporate CCTV systems	
	Assessment	Comments	Assessment	Comments
East Gippsland	Partly met	East Gippsland has a code of practice for its public safety CCTV system with useful content but no operating or procedures manual.	X	East Gippsland has not provided operating or procedure documents for the management of corporate CCTV systems. However, it does have detailed procedures to govern its drone program.
Horsham	X	Horsham has system network description documents for the Horsham Town Centre public safety CCTV system but no operating or procedures manual. It has a draft code of practice with useful content, but this has not been approved for use.	X	Horsham does not have site-specific user operating manuals for its corporate CCTV systems.

Source: VAGO based on assessment of council information.

Overall, we found a lack of comprehensive operating manuals to support CCTV policies. Most councils had detailed technical manuals provided by the suppliers of their CCTV systems. However, they have not complemented these manuals with site- and system-specific operating instructions detailing the councils' expectations and approved procedures for the management and use of these systems and the information they generate. This lack of detailed guidance increases the risk that council staff may not manage systems in accordance with PDPA and council policies.

2.3 Approval of surveillance devices

The use and extent of surveillance should be necessary, proportionate and for a legitimate council function. Councils should directly assess the potential impacts of proposed surveillance systems on the privacy of individuals and data security requirements when they consider installing a new surveillance system or adding to existing systems.

Councils should have a comprehensive process for assessing and deciding on whether to install surveillance devices in public places. This process needs to demonstrate robust consideration of the relevant Information Privacy Principles and guidance material described in Figures 1A and 1B.

CPDP's *Guidelines to surveillance and privacy in the Victorian public sector* indicate that surveillance operators must assess the privacy impacts of the proposed surveillance and consider consulting the community before the surveillance commences. OVIC provides an easily accessible template for privacy impact assessments.

The councils examined in this audit have long-established corporate CCTV systems and have predominantly added to existing systems over recent years rather than installing entirely new systems. We looked for evidence of explicit consideration of privacy implications and data security in council decision-making on the installation of additional corporate CCTV cameras and only found evidence at East Gippsland. There was only limited evidence of community consultation as part of such decisions at all councils examined.

East Gippsland was able to demonstrate that it has considered the privacy impacts associated with three of the five proposals since 2014 for new or upgraded corporate CCTV systems it provided documentation for. The council also has a sound CCTV assessment checklist to assist with the review of proposals for new CCTV systems. However, the council has not used this checklist to assess all proposals for new corporate CCTV systems.

At Horsham, there appeared to be no formal central approval process for the installation of corporate CCTV systems. Instead, systems were installed at the discretion of local facility managers. Horsham has not demonstrated that it considered any privacy impacts associated with the recent installation of CCTV cameras and equipment at a council-controlled childcare facility and aquatic centre.

2.4 Managing council CCTV systems

Councils have clear obligations to ensure that their use of CCTV and other surveillance devices complies with the law and respects the privacy of individuals.

Council policies on CCTV typically assign overall management responsibility to a senior council officer or department. In practice, corporate CCTV systems are dispersed across multiple sites. The local managers of these council offices, libraries, pools and other facilities play an important role in the day-to-day use and management of these corporate CCTV systems.

However, we found that, other than at Melbourne and East Gippsland, there was little, if any, routine central oversight of the management of these systems by council.

Regular reporting on key metrics for all corporate CCTV systems—for example, the number of times council staff review, save and copy CCTV footage and provide footage to external parties—would make senior management aware of these surveillance activities. This would promote more active management and support a culture of appropriate use.

Figure 2C shows our assessment of councils' management of corporate CCTV systems.

Figure 2C
Councils' management of corporate CCTV systems

Criteria	Melbourne	Whitehorse	Hume	East Gippsland	Horsham
Clearly assigned overall management responsibility for CCTV systems	✓	✓	✓	✓	✓
Responsible council area	Engineering	Shared	Governance	Shared	Technical Services
Evidence of active whole-of-council management approach to CCTV systems	✓	X	X	Partial	X
Regular management reporting on corporate CCTV systems	X	X	X	X	X
Standard minimum training package used	X	X	X	X	X
Agreements with contractors involved in managing, maintaining or supporting CCTV systems clearly articulate and reinforce privacy obligations	X	X	X	X	X

Source: VAGO based on assessment of council information.

Management responsibility

The responsibility for management oversight of surveillance devices is positioned in a range of departments at the five councils. We found little evidence of oversight by senior management of CCTV surveillance activities and systems, other than at Melbourne and, to a lesser extent, East Gippsland.

Melbourne

The Manager, Engineering Services, is responsible for authorising and overseeing the management of corporate CCTV systems. The Engineering Services department includes a specialist security services group responsible for managing the public safety and corporate CCTV systems and the council's other security technology and systems (such as building access, alarms and swipe cards). Responsibility for the day-to-day operation and management of corporate CCTV systems rests with local site or facility managers. The security services group demonstrated elements of whole-of-council oversight of the use of CCTV systems.

Whitehorse

The General Manager, City Development, owns the CCTV policy. The Engineering and Environmental Services department is responsible for the initial installation of CCTV systems and the council's Infrastructure Division is responsible for maintaining all CCTV systems. Responsibility for the day-to-day operation and management of corporate CCTV systems rests with local site or facility managers. There was no evidence of active whole-of-council oversight of the management of CCTV systems. The Infrastructure Division manages maintenance and functional issues but is not monitoring use of these systems.

Hume

The Manager, Governance, has overarching policy and oversight responsibility for the council's CCTV operations. Local council staff are responsible for day-to-day management of CCTV systems at individual facilities. The Engineering department manages maintenance and functional issues but does not monitor use of these systems.

East Gippsland

Management responsibility for CCTV systems is shared across several roles:

- The executive group assesses and approves requests for new public safety CCTV cameras and equipment.
- The Director, Corporate, owns the CCTV policy, decides on applications for access to recorded footage, and has overall responsibility for the effective and ethical management of equipment, ensuring that recorded information is appropriately maintained by authorised users.
- The Manager, Information Services, is responsible for overseeing the installation of approved CCTV monitoring equipment, for the ethical and effective management of CCTV equipment and systems and for ensuring that recorded information is appropriately maintained by authorised users. This role also oversees contracted equipment service providers working on the council's CCTV systems.
- The Governance and Compliance Coordinator receives and processes applications for access to recorded information for approval by the Director, Corporate. The Governance and Compliance Coordinator assists the CCTV project steering committee with the preparation of the annual public safety CCTV program review for presentation to the council's audit committee.

East Gippsland maintains central oversight and control of the operation of its corporate CCTV activities by limiting access to the systems to minimise the need for oversight. Very few sites allow for live monitoring. At all others, data is recorded on storage equipment which staff cannot access. The council's IT department is responsible for the day-to-day support and maintenance of CCTV systems and for extracting required footage from these systems.

Horsham

The Director, Technical Services, is responsible for overseeing the council's CCTV operations. Local council staff are responsible for day-to-day management of CCTV systems at individual facilities. The Technical Services department did not have a comprehensive list of all CCTV systems at the time of the audit. Technical Services manages maintenance and functional issues but does not monitor the use of these systems. The absence of strong policy and procedure documents and effective assurance mechanisms creates further risks.

Management reporting

We found no regular internal management reporting on the operation and management of CCTV systems at any of the audited councils. Regular reporting on key metrics for all council CCTV systems would make senior management aware of these surveillance activities, promote more active management, and support a culture of appropriate use.

Compiling a regular internal management report would not be an onerous administrative task and, if properly implemented, would be a strong control for identifying any suspicious or inappropriate use of council CCTV systems. A monthly or quarterly report could document:

- the number of incidents requiring review of CCTV footage
- how many times footage has been downloaded or copied and the reasons for this action—from CCTV system activity logs
- the number of requests for footage
- the number of complaints
- how many times footage has been released, to whom, for what reason, and who authorised the release
- a summary of maintenance issues.

Training

Staff involved in using and managing surveillance systems should be made aware of their individual obligations and understand how they should manage the information captured by surveillance activities to keep it secure and protect the privacy of any individuals recorded by the system. Councils should provide relevant employees with easily accessible policies and procedures and relevant training.

OVIC advises that providing training to staff is critical for ensuring that they are aware of their information-handling obligations under both internal organisational policies and PDPA. Further, it is a key element in promoting a consistent approach to protecting personal information.

The councils indicated that all new staff receive either face-to-face or online training covering privacy obligations and human rights as part of their induction. This is positive, but none of the councils could demonstrate that they had a training program specifically targeted at staff using CCTV systems covering privacy, appropriate use and data security requirements.

We found little evidence of comprehensive, standardised training for staff at local sites who manage CCTV systems. This is despite some councils including specific training commitments in their CCTV policies. Instead, staff participate in local training that focuses on the functional use of the system rather than privacy and data security.

We understand that, for practical reasons, training on the operation and use of CCTV systems may be developed and delivered locally at relevant sites. However, this brings with it a risk of inconsistency and that the local training does not adequately cover key content on privacy and data security.

Use of contractors

All councils use contractors to undertake routine maintenance of their CCTV systems, and some engage contractors to manage facilities with CCTV systems installed.

CPDP *Guidelines to surveillance and privacy in the Victorian public sector* makes it clear that organisations engaging a contracted service provider to manage all, or part of, their surveillance activities must ensure that the contract sets out the agreed governance arrangements and responsibilities for each party involved, including which party retains liability for privacy obligations under PDPA.

We checked the agreements in place at the audited councils and found few specific references to privacy and data security obligations relating to contractors' access to and use of CCTV systems. Figure 2D provides an example of a council's arrangements with a service provider involved in managing CCTV systems that illustrates this.

Figure 2D

Case study: Arrangement between the City of Melbourne and a contracted service provider

Melbourne engages a contracted service provider to manage a number of its recreational facilities. The service specification requires the service provider to comply with all relevant statutory or regulatory requirements, including privacy legislation.

Another clause requires the service provider to comply with all relevant council policies and procedures referred to in the contract as well as others that may be applicable to the service provider's operations. However, the council's CCTV management procedure is not referred to in the contract, and the section on managing the CCTV systems at these facilities does not detail clear minimum standards or expectations for the management and use of CCTV systems.

Source: VAGO based on information from Melbourne.

Cost

Councils should understand and consider the whole-of-life costs associated with installing and managing surveillance systems. While the councils could identify these costs, none were regularly tracking and monitoring them.

2.5 Arrangements with Victoria Police

Typically, councils install public safety CCTV cameras in known ‘hotspots’ for antisocial behaviour or crime, based on input from Victoria Police, local traders and the community. They also install CCTV monitors and recording equipment in a local police station so police can view, review and copy footage. Councils maintain the CCTV cameras, communications devices for these systems and the monitors and recording equipment at the police stations.

While councils own and are responsible for the information generated by the systems, they do not have direct access to the footage from the cameras. The exception to this is Melbourne where the council actively monitors its public safety CCTV cameras, 24 hours a day, seven days a week. The footage from these cameras is also transmitted directly to Victoria Police but it must contact the council to obtain copies of footage.

Victoria Police uses public safety CCTV systems based on operational needs but does not constantly monitor the CCTV cameras.

Memorandums of understanding

Public safety CCTV systems

Victoria Police’s stated policy position is that it will not access council CCTV information without having a formal MoU to govern its access to these systems. All of the audited councils have MoUs with Victoria Police to govern the operation and oversight of public safety CCTV systems. The only exception to this is Whitehorse which does not have an MoU for one of its three public safety CCTV systems.

The MoUs are comprehensive and follow a standard template with minor variations. They define the joint and individual responsibilities of each party and specifically require:

- both parties to only use the systems and their data, images and recordings for legitimate purposes
- both parties to take reasonable steps to protect the information collected by the systems from misuse and inappropriate disclosure
- councils to establish a steering committee and an audit committee to oversee the use of the systems and provide transparency to the community
- the steering committee to oversee the management of the system, develop a monitoring and evaluation framework and consider recommendations from the audit committee
- the audit committee to:
 - report annually to the steering committee on system management
 - ensure adherence to the MoU, the council’s CCTV policy and the law
 - promote public confidence by ensuring that the operation of the systems is transparent and open to public scrutiny
 - recommend any required improvements in the integrity of the systems

- councils to undertake regular and rigorous evaluation of the systems
- Victoria Police to keep a register of any images or recordings taken from the system and to give the council access to agreed data for the purposes of monitoring system use.

The MoU between Melbourne and Victoria Police is not as detailed as those at other councils, because Melbourne is responsible for monitoring and recording footage from its public safety CCTV system. Despite this, the MoU imposes the same or similar overarching obligations on the parties as those listed in the standard MoU template including to:

- comply with PDPA and the Safe City Camera Program public safety CCTV system operating manual
- responsibly operate and use the system
- securely store, distribute and destroy system information
- participate and cooperate in the management and oversight of the system, including in audits and evaluations.

Corporate CCTV systems

The audited councils do not have separate agreements with Victoria Police to guide provision of footage from corporate CCTV systems. Requests from Victoria Police for such footage are dealt with under the council's CCTV policies, where they exist.

Audit assessment

A robust MoU agreement is not sufficient on its own—councils need to implement the agreement and meet their obligations to provide proper oversight and accountability for the use of their CCTV systems.

We found most councils do not actively use their rights under the MoUs to review whether Victoria Police delivers on its commitments to record its usage of the systems and manage the data appropriately.

Apart from Melbourne, none of the councils have adequately used their agreements with Victoria Police to ensure proper oversight and accountability for the use of public safety CCTV systems. The common issues were councils:

- failing to establish the oversight committees required by the MoU
- establishing committees that meet rarely, do not focus on privacy and data security and do not perform the reviews and audits of police system use
- failing to monitor whether Victoria Police meets its appropriate use and data security obligations.

Appendix B shows our detailed assessment for the audited councils.

2.6 Improving oversight of public safety CCTV systems

There are a number of ways councils can improve their oversight of public safety CCTV systems.

Governance

Councils are responsible for establishing and supporting the governance structures that oversee public safety CCTV systems. Most can improve their performance by:

- meeting commitments made to establish steering and audit committees or assigning these roles to existing committees or governance groups that have the resources, time and expertise to fulfil them
- inviting other stakeholders and independent and/or specialist members to participate in steering and audit committees
- scheduling regular meetings of oversight committees with frequency based on workload and the extent and significance of issues to be addressed
- actively managing meeting agendas to move discussions at these oversight committees beyond operational and maintenance issues to comprehensively address the roles set for them in the MoUs and terms of reference
- better supporting the committees by providing written reports and evidence
- including a focus on privacy and data security.

Review of Victoria Police use

The audited councils need to exercise their right to obtain assurance about Victoria Police's appropriate use and management of the information provided by public safety CCTV systems. This includes by checking whether Victoria Police is comprehensively documenting details of copied images and recordings at local police stations. Any gaps in Victoria Police usage records increases the risk of privacy and data security breaches going unidentified and unaddressed.

Whitehorse agreement with Box Hill shopping centre owner

Whitehorse signed an agreement with the owner of Box Hill shopping centre in May 2011 in relation to the public safety CCTV system in the Box Hill mall and laneways. The agreement includes a CCTV management protocol and expires in March 2021.

The owner of the shopping centre, who have their own CCTV cameras inside the complex, agreed to allow Whitehorse to install public safety CCTV cameras and related recording and communications equipment on its premises. The owner's security contractors were the main operators of the system and provided footage to Victoria Police on request up until 2017 when Victoria Police was given direct access to view, copy and save footage from the system. The owner of the shopping centre retained access to the system and its footage following the provision of direct access to Victoria Police.

The agreement and protocol make it very clear that Whitehorse:

- owns the CCTV system, including all cameras and ancillary equipment and all data and images recorded by the system
- is responsible for the costs of maintaining, upgrading, moving or repairing the system
- cannot upgrade, add to or relocate cameras without consulting the shopping centre owner.

The agreement and protocol also make the shopping centre owner responsible for managing and operating the CCTV system and allows it to use the system and its recorded data for its own security management purposes. The company's obligations include:

- restricting access to the CCTV system and its data
- providing reports to the council on who accessed the CCTV system and recorded data
- ensuring its use of the system is legitimate and that it keeps any data that it copies from the system for its security management purposes secure and deletes this data when it is no longer needed
- not disclosing recorded data to any third parties other than Victoria Police and the council
- ensuring that only suitably qualified and licensed or registered persons are managing, operating and controlling the system
- training its staff in using the system
- maintaining a written report or log sheet recording requests from Victoria Police and the council to view or obtain copies of recorded data
- keeping records of the names of Victoria Police officers who are provided with copies of recorded data and details about the data provided
- directing all complaints and media enquiries about the system to Whitehorse
- complying with the Information Privacy Principles set out in PDPA even though it is not legally subject to them.

Whitehorse could not demonstrate that it has taken any steps to assure itself about the extent to which the shopping centre owner has met these obligations. For example, it could not provide evidence that it has sought access to the various reports and logs required under the agreement or tested the appropriateness of the owner's use of the system.

The shopping centre owner has cooperated with the council and Victoria Police and sent representatives to each of the four steering committee meetings since June 2014. However, there is little evidence that the council uses these meetings to test compliance with the agreement. It is unclear what arrangements Whitehorse had in place prior to the formation of the Box Hill Safety and Security Steering Committee to monitor the shopping centre owner's operation of the system including its handling of recorded data.

We visited the security control room as part of this audit. The representative of the shopping centre owner's security contractor was not familiar with the agreement and protocol. The council-owned recording equipment and monitor are in an open area. We saw evidence that this security contractor keeps a log of CCTV footage provided to Victoria Police, but this log does not record whether the footage was from the council's cameras or the shopping centre cameras.

The council installed a fibre-optic link between the CCTV equipment in the shopping centre and the Box Hill police station in 2017. This link means that Victoria Police can now monitor the CCTV cameras live from the police station and access the recording system to copy required footage. Victoria Police no longer needs to attend the shopping centre security control room to obtain copies of footage.

Whitehorse has advised that it intends to remove its CCTV recording equipment from the shopping centre owner's premises.

2.7 Governance, assurance and accountability

Councils should establish a framework and process to ensure they regularly scrutinise their surveillance activities against their intended purposes, the law and approved policies and procedures. Audits, reviews or evaluations should be independent of program management and the results reported to the community.

Councils can assign this oversight role to a separate, specialist oversight or audit committee or to an existing council committee or governance group. Members could include people with relevant expertise, community representatives and key users such as Victoria Police, but should not include members involved in the day-to-day management of surveillance systems.

In section 2.5, we examined the adequacy of governance, assurance and accountability arrangements for public safety CCTV systems. This section focuses on corporate CCTV systems.

None of the councils could demonstrate that their audit committee or a specialist oversight committee regularly scrutinises the council's management and use of corporate CCTV systems. This is despite Whitehorse and Hume committing to do this in policies and other public documents.

There are many more council-managed corporate cameras than public safety cameras and, arguably, greater privacy and data security risks, because these cameras are dispersed across many locations and subject to local operating practices. This, combined with little evidence of specific central oversight or management of the use of corporate CCTV systems at Whitehorse, Hume and Horsham, makes it difficult for these councils to demonstrate compliance with relevant legislation and proper management of CCTV systems and data.

In addition, none of the councils carry out regular assessments on whether their management and use of surveillance devices is consistent with their intended purposes, the law and approved policies and procedures. The few reviews we saw evidence of were focused on functionality rather than appropriateness of use.

There is also no public reporting on the use of corporate CCTV systems by any of the audited councils, meaning the use of the vast majority of these systems is not routinely scrutinised. Ideally, councils should report periodically to councillors and the community on compliance with key legal, policy and procedure requirements for their surveillance activities.

Figure 2E shows our assessments of the audited councils' governance and oversight arrangements.

Figure 2E
Councils' governance and oversight arrangement for corporate CCTV systems

Council	Assessment	Comments
Melbourne	X	<p>Melbourne does not have a specialist oversight committee for its corporate CCTV system, and there is no evidence of any coverage of the system's use by the council's audit committee.</p> <p>The council has no regular audit or assurance mechanisms over the operation of its corporate CCTV system.</p> <p>Melbourne does not report publicly on the protection of privacy and data security for information captured by its corporate CCTV systems.</p>
Whitehorse	X	<p>Whitehorse's CCTV policy indicates that the council's risk management committee will perform the audit and risk committee's role in overseeing the management, use and integrity of the council's corporate CCTV systems. However, Whitehorse has not provided any evidence that these oversight mechanisms are operating.</p> <p>The council's CCTV policy states that there will be appropriate and ongoing monitoring and evaluation of CCTV systems to ensure that:</p> <ul style="list-style-type: none"> CCTV systems comply with relevant legislation and other laws management of CCTV records/footage is appropriate, including its use, retention, security, privacy, access, disclosure, storage and disposal. <p>Despite these clear commitments, we found no evidence of ongoing assessment, audit or evaluation of the operation and effectiveness of Whitehorse's CCTV systems.</p> <p>Whitehorse does not report publicly on how it protects the privacy and data security for information captured by its corporate CCTV systems.</p>

Figure 2E

Councils' governance and oversight arrangement for corporate CCTV systems—*continued*

Council	Assessment	Comments
Hume	X	<p>Despite public and other commitments to undertake regular reviews and audits of the operation and management of CCTV systems, Hume has not performed any such audits or reviews.</p> <p>Hume commissioned a technical/functional review of its corporate CCTV systems in early 2018. The scope of this review did not extend to examining privacy and data security or appropriateness of use.</p> <p>Hume does not have a specialist oversight committee and provided no evidence of substantive oversight of its corporate CCTV systems by the council's audit committee. Hume advised that the audit committee's charter does not specifically identify CCTV operations as an issue for oversight but that the committee assess this indirectly as part of the overall risk review and monitoring of council's operations. In planning for the next three-year internal audit plan, council management intends to discuss with the audit committee the merits of including a review of CCTV operations and risks.</p> <p>The CCTV policy is silent on any other regular review or assurance processes to test compliance with the policy. We asked whether there are any such reviews in place covering the public safety CCTV system installed in Sunbury or corporate CCTV systems. Hume advised that it has not undertaken a review or audit but that it intends to introduce compliance checking for corporate CCTV system use and include an audit in its three-year internal audit program.</p> <p>Hume does not report publicly on the protection of privacy and data security for information captured by its corporate CCTV systems.</p>
East Gippsland	X	<p>There is no oversight committee to review the operation of East Gippsland's corporate CCTV systems.</p> <p>The council does not undertake regular reviews, audits or assessments to obtain ongoing assurance about whether its management and operation of corporate CCTV systems complies with the law and the council's expectations. The council has not committed to do so.</p> <p>East Gippsland did commission a review of its corporate CCTV systems in early 2016 to assess the condition of its CCTV assets and its physical and IT security. The council resolved some immediate issues highlighted in that review, such as changing passwords and resolving remote access where possible and identified that significant investment was required to upgrade the systems and allow for better access controls, audit logging and replacement of cameras with appropriate equipment.</p> <p>The council approved a budget bid for the 2018–19 financial year to enable a full review of the operation and management of the corporate CCTV systems as the council updates the infrastructure and centralises access.</p> <p>East Gippsland does not report publicly on the protection of privacy and data security for information captured by corporate CCTV systems.</p>
Horsham	X	<p>Horsham does not have a steering committee for its corporate CCTV systems.</p> <p>The council has not taken any steps to obtain ongoing assurance about whether its CCTV surveillance activities comply with relevant legislation and council policies and requests.</p> <p>Horsham does not report publicly on its corporate CCTV surveillance operations.</p>

Key: X means there is no oversight committee, no regular audits of appropriate use, no evaluations against objectives and no public reporting on the management and use of corporate CCTV systems.

Source: VAGO based on assessment of council information.

3

Privacy and data security

Councils should maintain adequate security over personal information recorded using surveillance technologies by complying with relevant data security and records management requirements. Under Information Privacy Principle 4 on data security, councils must take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure.

Effective data security involves:

- ensuring physical security over surveillance devices and equipment
- having security controls on the ICT used in the devices and equipment
- limiting access to surveillance footage and records to council staff and contractors with a need to know, and law enforcement officers
- taking steps to deter and detect security breaches.

This part of the report focuses on whether the audited councils adequately manage privacy issues and can demonstrate data security for their corporate and public safety CCTV surveillance systems.

3.1 Conclusion

The audited councils have not identified any inappropriate use of their surveillance systems or footage, and OVIC advised that it has never received a complaint about such use. This is positive, and we found that the councils have good awareness of the privacy issues associated with the use of CCTV systems.

However, all five councils can improve the security of the personal information they gather through their CCTV systems, to better protect the privacy of individuals. Key areas to address include improving physical security and access controls for corporate CCTV systems and regularly assessing whether controls are working.

The audited councils all use generic and shared user logins for corporate CCTV systems. Some do not require staff to record their reasons for accessing CCTV footage or do not use system activity logs to track usage. These practices increase the risk of inappropriate use occurring and going undetected. There are similar issues with public safety CCTV systems.

Improving physical security and access controls will better enable the councils to ensure appropriate access to and use of these systems. This will help councils ensure that the information collected from councils' surveillance activities in public places is protected from unauthorised disclosure.

In addition, we found at least one site at each council where CCTV operates in public spaces without adequate public signage.

3.2 Collection, information and signage

Information Privacy Principle 1 requires councils to only collect personal information that is necessary and lawful, and to do so with as little intrusion as possible.

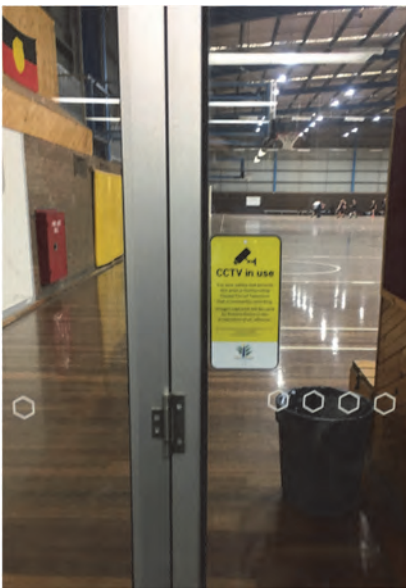
Councils collecting personal information must also take reasonable steps to ensure that individuals are aware of:

- the identity of the council
- the purpose for which the information is collected
- the fact that the individual is able to access the collected information
- who the council usually discloses the information to.

We expected the councils to comply with Information Privacy Principle 1 by:

- taking reasonable steps, such as installing signage, to make people aware that surveillance devices are in use in public places and where they can obtain further information
- making their policies and other information on the use of surveillance systems easily accessible to the community.

Figure 3A summarises the results of our assessments of the councils' compliance with Information Privacy Principle 1. We reviewed their publicly available policy and other information on their CCTV surveillance activities. We also visited a sample of sites at each council to see whether there was adequate signage advising the public that the areas were under CCTV surveillance.



Example of good CCTV signage at the entrance to a council sports centre.

Figure 3A

Compliance of councils' CCTV surveillance with Information Privacy Principle 1

Criteria	Melbourne	Whitehorse	Hume	East Gippsland	Horsham
Stated purpose(s) for collecting information using CCTV systems related to legitimate, lawful functions	✓	✓	✓	✓	✓
Adequate signage in all public places under CCTV surveillance, for both public safety and corporate systems	X	X	X	X	X
Easily accessible policies or other information covering all CCTV use that describes:	X	✓	✓	✓	X
• the purpose for collecting information by CCTV	Public safety CCTV only	✓	✓	✓	X
• how individuals can seek access to collected information	Public safety CCTV only	✓	✓	✓	X
• to whom the council usually discloses the information	Public safety CCTV only	✓	✓	✓	X

Source: VAGO based on review of council information.

Collection and use

The primary reasons councils engage in CCTV surveillance in public places include:

- improving actual and perceived levels of public safety by discouraging unlawful and antisocial behaviour in and around council property, facilities and public places
- assisting Victoria Police with the detection and prosecution of offences
- monitoring areas where council staff interact with the public to enhance safety
- protecting council assets by discouraging theft or misuse
- deterring and reducing graffiti and other forms of vandalism
- enabling real-time review of material entering council waste management facilities.

These are legitimate reasons that relate directly to council purposes under the *Local Government Act 1989*.

Signage

Signs in public places under CCTV surveillance should:

- clearly state that the area is under surveillance and identify the organisation undertaking surveillance
- be located before the CCTV surveillance starts, to enable individuals to make a choice about whether to enter the areas under surveillance.

For councils' public safety CCTV systems, it was positive to find easily identifiable signage in place for the majority of CCTV sites at all councils. However, Whitehorse needs to improve the visibility of signage at the Box Hill mall.

For councils' corporate CCTV systems, we found sites with absent or deficient CCTV surveillance signage at every council. The common gaps and deficiencies in corporate CCTV signage were:

- no signage in place
- signage in place but not easily seen
- signage in place, but not positioned well enough to warn the public of CCTV before the surveillance commenced
- signage not identifying the council operating the CCTV system and/or not providing contact information.

Hume and Whitehorse include specific commitments to ensure there is adequate signage in their publicly available policies on CCTV, but they have not always met these commitments at corporate CCTV sites. Hume has recently taken action to address signage gaps at 19 sites with corporate CCTV systems.

East Gippsland uses a drone to examine locations where physical access by council staff is restricted by distance, danger or difficult terrain for activities like examining sand movement in coastal areas to inform dredging. The council is careful to provide adequate notice to residents and other members of the public through direct letter drops, advertisements in the local media, or notices on its website advising where and when the drone will operate. East Gippsland do not use its drone for surveillance activities.

Public information on purpose, access and disclosure

We assessed whether the audited councils provided easily accessible policies or other information to the public covering both their public safety and corporate CCTV systems.

We found that only Whitehorse and Hume provide easily accessible information to the public covering all of their CCTV systems, describing:

- the purpose for collecting information by CCTV
- how individuals can seek access to the collected information
- who the council usually discloses the information to.



Example of good CCTV signage in a public park.

East Gippsland makes its CCTV policy publicly available and it covers purpose, access and disclosure. However, this policy primarily deals with the public safety CCTV system.

Horsham is yet to develop a policy on its use of CCTV surveillance and does not make any other information on public safety or corporate CCTV system use easily accessible to the public.

Melbourne has not made its policies on public safety and corporate CCTV system use accessible to the public, but provides information that covers purpose, access and disclosure on the public safety CCTV system as part of its Safe City Camera Program on its website.

3.3 Data security

Data security is a critical component of any surveillance program. Public sector organisations have an obligation to protect the personal information they hold from being misused, lost, accessed, modified or disclosed by unauthorised persons.

Information security classification

OVIC advises councils that the best way to comply with Information Privacy Principle 4 is to comply with the VPDSF.

The VPDSF requires public sector entities to:

- identify their information assets
- determine the value of their information assets
- identify any risk to their information assets
- apply security measures to protect their information assets
- manage risks across the information life cycle.

Given this, we expected to find that councils had applied an information or data classification rating to the information they gathered through their CCTV systems and designated required handling requirements for this information, such as classification labelling, and encryption of data stored and transferred from one point to another.

We found that none of the councils had assessed and documented an information security classification for surveillance information. However, we did not note any reported incidents of the mishandling of the surveillance data.

In the absence of the information security classification rating, there is a risk that councils may not handle information appropriately to ensure the reasonable security of CCTV data throughout its life cycle.

Physical security

Ensuring the physical security of the equipment used to capture and store CCTV footage minimises the risk of unauthorised access and tampering or data theft. Figure 3B summaries our assessment of the physical security of councils' CCTV systems.

Figure 3B
Physical security of councils' CCTV equipment for corporate CCTV systems

Criteria	Melbourne	Whitehorse	Hume	East Gippsland	Horsham
Corporate CCTV systems					
CCTV storage devices hosted in a secured rack or cabinet	X	✓	✓	X	X
Rack/cabinet always locked	X	✓	X	X	X
Rack or cabinet hosting storage equipment is segregated from the staff workspace	X	X	✓	X	X
Workspace accessible only by authorised personnel	✓	X	✓	X	X
Public safety CCTV systems					
CCTV storage equipment hosted in a secured rack or cabinet	✓	✓	✓	✓	✓
Rack/cabinet always locked	X	X	X	X	X
Room hosting rack or cabinet is segregated from the staff workspace:	✓	X	✓	✓	✓
• room hosting rack or cabinet always locked	✓	✓	✓	✓	✓
• room accessible only by authorised personnel	✓	X	✓	✓	✓

Source: VAGO based on review of council information.

Corporate CCTV systems

Overall, we found that councils did not consistently apply physical security controls for their corporate CCTV systems' storage devices. Where there are weak physical security controls over the equipment storing CCTV data, there are data security risks such as access by unauthorised personnel.

During our site visits, we also observed inadequate environmental controls at some of the sites—see Figure C2 in Appendix C. Examples included the storage of cardboard boxes and construction material in the same place, dusty environments, and inadequate temperature and moisture control. Inadequate environmental controls increase the risk of equipment failure which may result in unexpected unavailability and data loss.

For most of the larger sites, CCTV data storage equipment is kept in a rack or cabinet. These racks or cabinets are specifically designed to provide proper physical and environmental conditions to host CCTV data storage equipment. However, this was not typically the case at smaller sites. At sites with less than four cameras, storage equipment is either kept openly in the staff work area or next to the monitors at the front desk, increasing the risk that equipment may be accessed by unauthorised personnel.

Of the councils we examined, only Whitehorse always locked the racks hosting the CCTV storage equipment. We found that Melbourne, Whitehorse, Horsham and East Gippsland do not segregate the cabinet hosting the equipment from the main work area.



CCTV system cabinet hosted in the maintenance room for a public toilet in a dusty environment without any temperature or humidity controls.



Network Video Recorder equipment kept in an unlocked rack with disorganised cabling.

Public safety CCTV systems

We visited four Victoria Police stations hosting server equipment for storing data from public safety CCTV systems, as well as the storage facility for data from Melbourne's public safety CCTV system. We did not find significant weaknesses in the physical security controls at these sites.

We found that all the police station sites we visited and the Melbourne public safety CCTV system site hosted the data storage equipment in lockable racks located in lockable rooms. However, none of these racks were locked. These racks were usually located in a room with other ICT equipment. This other equipment is maintained by service providers not authorised to access the CCTV storage equipment, creating the risk of unauthorised access to this equipment.

At Whitehorse, we found significant issues with physical security, including:

- one site where the CCTV storage rack is located in the maintenance area of a public toilet
- another site where the rack is located in the main work area of the security office of a shopping centre.

Neither of these racks were locked, meaning maintenance or other personnel with access to these locations can gain unauthorised access to the equipment, creating a risk to the system and data security.

ICT access controls

Access controls are the ICT security controls that councils implement to prevent unauthorised access and protect the confidentiality, integrity and availability of the information they process and store electronically. Key access controls for CCTV systems include restricting user access, enforcing the use of passwords, performing periodic user access reviews and monitoring access to the system regularly.

Overall, we found that the audited councils had reasonable restricted access controls for CCTV systems, to ensure that footage is viewed and downloaded only by appropriate personnel. However, we also identified some gaps which may present a risk to data security—see Figure 3C.

Figure 3C
Councils' access controls for CCTV systems

Criteria	Melbourne	Whitehorse	Hume	East Gippsland	Horsham
Corporate CCTV systems					
Password in place	✓	✓	✓	✓	✓
Enforced strong password policies as per the council's corporate policies	X	X	X	X	X
Identifiable user logins in place (no shared or generic logins used)	X	X	X	X	X
Assigned logins have role-based access (restricted to view and download footage)	✓	✓	✓	✓	✓
Periodic user access reviews are performed:	X	X	X	X	X
• administrative privileges are restricted	✓	✓	✓	✓	✓
• user activity audit logging enabled	X	X	✓	X	X
• user activity audit log reviewed	X	X	X	X	X
Public safety CCTV systems					
Password in place	✓	✓	✓	✓	✓
Enforced strong password policies as per the council's corporate policies	X	X	X	X	X
Identifiable user logins in place (no shared or generic logins used)	✓	X	X	X	X
Assigned logins have role-based access (restricted to view and download footage)	✓	✓	✓	✓	✓
Periodic user access reviews are performed:	X	X	X	X	X
• administrative privileges are restricted	✓	✓	✓	✓	✓
• user activity audit logging enabled	✓	X	✓	X	X
• user activity audit log reviewed	X	X	X	X	X

Source: VAGO based on review of council CCTV sites.

We found gaps in all councils' access controls for both their corporate and public safety CCTV systems:

- Councils use generic and shared user logins for staff who require access to view and download CCTV footage. The use of generic and shared logins increases the risk that inappropriate use of the system will not be traceable to a specific employee.
- Councils do not perform periodic user access reviews to ensure only staff who need access to CCTV footage have it.
- There is no documented process detailing how to provide and remove user access. However, we observed that administrator privilege access is limited to authorised users.
- Password settings such as minimum password length, complexity and expiry dates are not always enforced, sometimes due to system limitations. We did not find any instances of blank passwords.
- Councils do not consistently configure their audit logging of user activity such as viewing and downloading CCTV footage. In addition, there is no policy and procedure requiring targeted reviews of user activity logs. These reviews could help councils to identify unusual or inappropriate activity, but they do not perform them.

Patching and updating CCTV systems

Patches are an additional piece of software released by vendors to fix security vulnerabilities or operational issues in existing software. Scheduled patching aims to reduce the risk of security vulnerabilities, which could be subject to malware and virus attacks. When patches are not applied regularly, known security vulnerabilities remain and are vulnerable to cyber-attack. This may result in unauthorised access to systems and data, and an increased risk to data security and privacy.

The audited councils did not perform any routine updates or patching for their corporate and public safety CCTV systems. As shown in Figure 3D, it has been several years since the councils last applied patches or system updates to their CCTV software.

Figure 3D
Councils' last patches/updates to installed public safety CCTV software

Council	Date of last patch/update
Melbourne	2015
Whitehorse	2017
Hume	2014
East Gippsland	2013
Horsham	2017

Source: VAGO based on information from the councils.

We found that none of the councils have upgraded the digital video recorders or network video recorders for their corporate CCTV systems since the initial installation and that different versions of the software exist at different facilities. The failure to upgrade this software increases the risk that any known security vulnerabilities in this software may expose the system to unauthorised access.

The smaller sites in Horsham, Melbourne, East Gippsland and Hume have video recorder software versions released in 2011–12. At East Gippsland, this equipment is configured to allow restricted remote access over the internet.

Backup management and disaster recovery planning

Backup management and disaster recovery planning involves councils identifying their business continuity requirements and data backup needs. Data is backed up or replicated on a regular basis to ensure data is securely available if there is a system outage or failure, or loss of data.

A business continuity plan details a council's response strategy to enable it to continue operating and minimise the impact to services in the event of a disruption. An IT disaster recovery plan is a documented process to assist the council to recover its IT infrastructure in the event of a disaster.

None of the councils have data backup policies covering corporate and public safety CCTV systems, because the councils do not categorise these systems as critical.

Currently, corporate and public safety CCTV systems are configured to record a maximum of 30 or 31 days of live footage data. There is risk this data will be lost if the data storage equipment fails. If a major incident occurred and the CCTV footage was not available, this loss of data and any related system unavailability may result in a reputational risk for the councils.

The absence of backup management and disaster recovery planning may also adversely impact the councils' ability to recover their CCTV systems and transactions in a complete and timely manner.

Records management

Councils should delete information gathered through surveillance activities once it is no longer required. This is consistent with PDPA and requirements set by PROV.

PROV sets retention and disposal authorities that public sector organisations, including councils, are required to comply with. Under disposal authority PROS 07/01 VAR 4 *Retention and Disposal Authority for Records of Common Administrative Functions*, issued March 2017, surveillance footage is classified as temporary, meaning it can be destroyed after its administrative use has ended. If footage is required to be kept, then the usual public sector record retention requirements apply.

Information Privacy Principle 4, concerning data security, requires councils to take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

Councils' CCTV equipment is programmed to overwrite the data after 30 or 31 days.

3.4 Use, disclosure and access

Surveillance footage and records should generally only be used and disclosed in accordance with the primary purpose of its collection such as enhancing public safety and discouraging theft or vandalism.

Information Privacy Principle 2 requires public sector organisations, including councils, to not use, or disclose to third parties, any personal information gathered on individuals for a purpose other than the primary purpose of collection, unless certain circumstances apply. These circumstances include instances where:

- the secondary purpose is related to the primary purpose of collection, and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose
- the individual has consented to the use or disclosure
- the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to an individual's or the public's life, health, safety or welfare
- the organisation has reason to suspect unlawful activity and uses or discloses the personal information to further its investigation or to report its concerns to relevant persons or authorities
- the use or disclosure is required or authorised by law
- the organisation reasonably believes that the use or disclosure is reasonably necessary to a law enforcement agency for a range of specified reasons such as the prevention, detection, investigation, prosecution or punishment of criminal offences
- the Australian Security Intelligence Organisation or the Australian Secret Intelligence Service has asked the organisation to disclose the personal information.

Information Privacy Principle 2 requires organisations who use or disclose personal information for law enforcement purposes to document that use or disclosure.

Information Privacy Principle 6 supports the rights of individuals to seek access to the personal information a council or other public sector agency holds about them, including CCTV surveillance footage. An organisation can deny access where disclosing the information would have an unreasonable impact on the privacy of other individuals, be unlawful or prejudice law-enforcement activities. Councils assessing requests for access to CCTV footage from an individual need to consider whether providing access would infringe the privacy of any other individuals captured in the footage.

It is important to note that the councils' capacity to use, disclose and provide access to surveillance footage is limited to the footage available to them. This is determined by the storage capacity of the equipment they use to record footage from CCTV systems, the camera settings and the extent to which they have saved specific footage. CCTV storage equipment is configured with either:

- a standard 'write over' period, typically 30 days, after which previously stored footage is recorded over and replaced by more recent footage on a continuous cycle
- a dynamic 'write over' period determined by the storage capacity of the equipment and the volume of recorded footage, influenced by settings for the CCTV systems—for example, whether they are continuously recording or only record when they detect motion.

If councils wish to retain footage, they need to extract and save it to another location before it is overwritten by their CCTV systems.

Public safety CCTV systems

Only Melbourne controls the footage recorded from its public safety CCTV system, because the control room that houses its storage equipment is in a council building.

Melbourne has strong controls over the access to and release of CCTV footage from its public safety CCTV system to Victoria Police, other third parties and individuals. It keeps a register of access and disclosure granted and a master copy of all footage released.

Apart from Whitehorse's public safety CCTV system housed at the Box Hill mall shopping centre—see the case study in Section 2.6—the other audited councils house their public safety CCTV systems storage equipment in local Victoria Police stations. Victoria Police controls the footage from these systems and determines what, if anything, to save and disclose to individuals, the public and the media. This audit did not examine Victoria Police's processes for using and disclosing CCTV footage from public safety systems.

Whitehorse, East Gippsland and Horsham refer requests from individuals and other third parties for access to public safety CCTV system footage to Victoria Police. Hume deals with these requests using its freedom of information process.

Corporate CCTV systems

The councils advised that there are occasional requests from Victoria Police for access to corporate CCTV system footage, as well as a small but increasing number of requests from individuals.

All councils provide access to and copies of footage from their corporate CCTV systems in response to requests from Victoria Police. They only rarely provide footage to the media and typically assess requests from individuals for access to CCTV footage under their freedom of information processes. Requests from individuals are almost always denied as providing access would impinge the privacy of other members of the public captured in the footage.

We examined how the councils manage access and disclosure of footage from their corporate CCTV systems and found strong controls at Melbourne and East Gippsland. We did find, however, one incident at East Gippsland that exposed weaknesses in the council's controls over the disclosure of footage. In May 2018, the council identified that some staff at two sites with corporate CCTV systems could access, review and extract copies of CCTV footage from those sites. The council addressed this issue quickly.

Melbourne maintains an incident management system for its corporate CCTV systems and documents requests for access to footage and the outcome of those requests. The process for obtaining copies of footage from these systems is tightly controlled. We were satisfied that Melbourne maintains adequate controls over the release of CCTV footage to Victoria Police and other third parties and individuals.

East Gippsland's processes authorise only two designated IT staff to extract copies of footage from corporate CCTV systems, and a register documents footage extracted from these systems in response to requests from council staff and the police. This provides a robust control environment.

Hume keeps a central register of video footage extracted from corporate CCTV systems in response to requests from Victoria Police and for other purposes.

Whitehorse and Horsham have less well-established processes and controls over the disclosure of footage from corporate CCTV systems to Victoria Police and others. These councils do not have a single comprehensive register of footage from their corporate CCTV systems provided to Victoria Police or other parties. Requests are most commonly received from Victoria Police and these are usually handled by the managers of the relevant sites. These managers review and save relevant CCTV footage and provide copies of still images and footage to Victoria Police on request. While this is appropriate, to fully comply with Information Privacy Principle 2 these councils need to keep a register of all such material provided to Victoria Police from all sites.

Appendix D shows our detailed findings on use, disclosure and access.

3.5 Inappropriate use

Councils should clearly document their expectations for appropriate use of CCTV systems by staff and have robust processes to address breaches of relevant laws and policies, including the misuse of the CCTV systems and footage.

All councils other than Horsham have a documented CCTV policy or procedure that covers expectations about appropriate staff use of CCTV systems, along with processes for dealing with inappropriate use. This means there are clear expectations for staff at these four councils.

Councils can mitigate the risks of inappropriate use of CCTV systems by restricting access to these systems to a limited number of authorised staff with a legitimate operational reason to have access. We found evidence that the audited councils make efforts to restrict access to relevant staff. However, the issues raised in Section 3.3 about the inadequacy of access controls, including the use of generic user logins to CCTV systems create risks that:

- unauthorised staff may access CCTV systems using these generic user login details
- councils will not be able to identify the individual staff members responsible for inappropriate use of the systems.

In addition, failure to log user activity can increase the risk that councils may not detect inappropriate use. CCTV system software typically has the capability to log all user activity—for example, users reviewing and copying or exporting CCTV footage. However, not all councils had enabled this feature and, where it was enabled, it was not routinely used to assess the appropriateness of use.

None of the councils could demonstrate any regular processes or procedures for detecting inappropriate or unauthorised access to, use or disclosure of CCTV systems by council staff or third parties. These processes could include routine, periodic reconciliation of user activity logs on CCTV system software against records kept by staff of access to CCTV information and footage.

At Horsham, we found that footage from the 21 CCTV cameras installed in the Children's Hub childcare facility could be remotely accessed by the council's Building Management department. This department oversaw the design and construction of this relatively new facility, but it is not clear why it requires ongoing access to CCTV footage from this facility.

At Melbourne, the risk of inappropriate use of the public safety CCTV system is largely mitigated. The council has a number of mechanisms in place to detect inappropriate use of the system, including:

- always having two operators in the public safety CCTV system control room
- streaming footage live to two police stations and the Victoria Police Operations Centre
- keeping the control room under constant CCTV surveillance.

3.6 Complaint handling

Councils should inform their communities of their right to make a complaint about the use of surveillance technologies. Councils should assess any complaints received using established complaints-handling processes.

We examined whether the councils have:

- policies advising the public on how to make a complaint about the presence or use of CCTV
- documented procedures on how to process and handle complaints
- received any complaints about CCTV.

Melbourne, Whitehorse and East Gippsland provide specific, publicly accessible information on how an individual can make an enquiry or complaint about the council's use of CCTV systems. This information is included in the council's publicly available CCTV policy, or on the council website section dealing with CCTV. Hume and Horsham have not provided the public with specific information on how to make complaints about their use of CCTV.

Even in the absence of specific policies for CCTV-related complaints, all of the audited councils have policies for general feedback and complaints made by the public about council activities, including CCTV surveillance. These policies are publicly available on council websites and provide information on how the public can lodge complaints with the council and time lines for handling complaints.

The councils also have publicly available privacy policies that apply to all personal information they hold, including any information collected through councils' CCTV systems. These policies include information on how individuals can lodge enquiries or complaints on the treatment of their personal information.

All five councils advised that they have not received any complaints on the presence or use of CCTV systems in the last five years.

Appendix A

Audit Act 1994 section 16— submissions and comments

We have consulted with Melbourne, Whitehorse, Hume, East Gippsland and Horsham, and we considered their views when reaching our audit conclusions. As required by section 16(3) of the *Audit Act 1994*, we gave a draft copy of this report, or relevant extracts, to those agencies and asked for their submissions and comments. We also provided a copy of the report to the Department of Premier and Cabinet.

Responsibility for the accuracy, fairness and balance of those comments rests solely with the agency head.

Responses were received as follows:

Melbourne	58
Whitehorse	62
Hume	64
East Gippsland	66
Horsham	72

RESPONSE provided by the Chief Executive Officer, Melbourne

11 September 2018



CITY OF MELBOURNE

GPO Box 1603
Melbourne VIC 3001

Phone 61 3 9658 9658
Fax 61 3 9654 4854
www.melbourne.vic.gov.au

DX210487
ABN 55 370 219 287

Mr. Andrew Greaves
Auditor-General
Level 31/ 35 Collins Street
Melbourne 3000

Dear Mr Greaves

AUDIT REPORT - SECURITY AND PRIVACY OF SURVEILLANCE TECHNOLOGIES IN PUBLIC PLACES

Thank you for forwarding to me a copy of the report entitled 'Security and Privacy of Surveillance Technologies in Public Places'.

As noted in your report, there are two categories of closed circuit television (CCTV) equipment managed by the City of Melbourne. These are:

1. Public systems installed under the Safe City Camera Program (SCCP) that proactively monitor the public space 24 hours each day.
2. Corporate systems installed within and outside the immediate environs of Council owned and/or managed buildings that are not proactively monitored but record activity that can be viewed later if an incident or offence has occurred.

Ensuring the highest levels of privacy protection is extremely important to Council, and there will always be a need for continuous improvement in this area.

The City of Melbourne has, at this date, not identified any incidents of inappropriate use of surveillance systems or footage. In addition the Office of the Victorian Information Commissioner has not received any complaints.

The priority of the City of Melbourne has been on the integrity and operational effectiveness of the Safe City Camera Program (SCCP) and your audit shows the effectiveness of these efforts.

However the City of Melbourne readily concedes that there are always opportunities for improvement in systems and processes and accepts the recommendations of the Audit Report. Please find attached a copy of our response to the recommendations including a timetable for implementation.

RESPONSE provided by the Chief Executive Officer, Melbourne—continued

If you would like to discuss this issue further, please contact Jenny Bailey, Manager Engineering Services on 9658 8533.

Yours sincerely

A handwritten signature in blue ink, appearing to read 'B. Rimmer', with a long horizontal flourish extending to the right.

Ben Rimmer
Chief Executive Officer

CoM reference: 11886342

ATTACHMENT ONE – RESPONSE TO RECOMMENDATIONS

No	Recommendation	Response	Timeframe
1	Review and update CCTV policies to address the requirements of the Privacy and Data Protection Act 2014.	No review and update is required for the Safe City Camera Program (SCCP) The City of Melbourne will review its Corporate CCTV Security Procedure Manual and ensure that the Manual fully addresses the requirements of the Privacy and Data Protection Act 2014.	March 2019
2	Assess all CCTV systems installed before the approval of a CCTV policy to ensure they comply with the policy.	This recommendation refers to our corporate systems not the SCCP. For corporate systems the City of Melbourne will ensure that all new CCTV installations also comply with its amended policies and procedures.	On-going
3	Assess the privacy impacts of proposals to install new or additional CCTV surveillance devices in public places.	Locations for SCCP are provided by Victoria Police. We will amend our Corporate Procedure CCTV Security Manual to reflect this recommendation.	December 2018
4	Develop site-specific operating procedures for their corporate CCTV systems to reflect the requirements of the Privacy and Data Protection Act 2014 and their policies.	The City of Melbourne will review its procedures for use at each corporate CCTV site including oversight and audit arrangements, contract management, training, reporting, records management, detailed operations and evaluation.	Commencing September 2018

RESPONSE provided by the Chief Executive Officer, Melbourne—continued

No	Recommendation	Response	Timeframe
5	Allocate responsibility for overseeing the operation of CCTV systems to an appropriate senior manager and implement regular reporting on key aspects of CCTV system use.	This is already in place for the SCCP. This will be extended to our corporate program.	December 2018
6	Include a periodic audit of CCTV system use and data security in their forward internal audit programs.	This is already in place for the SCCP. The City of Melbourne will institute a periodic audit process for corporate CCTV systems.	Ongoing
7	Review and update the content and position of all signage in locations with corporate CCTV systems to reflect better practice.	All corporate sites will be reviewed and signage installed or updated in locations that allow people to understand the presence of CCTV before they enter a building.	Commencing February 2019
8	Review and address access control and data security weaknesses for corporate CCTV systems.	Access control and data security will be reviewed as part of a site by site audit and review of our corporate CCTV systems.	Immediate priorities will be assessed and work undertaken. Site specific assessments will commence in August 2019
9	Ensure regular audits and evaluations of public safety CCTV systems and hold the oversight committees for these systems to account for meeting their responsibilities under agreements with Victoria Police.	This is already in place for SCCP.	N/A

RESPONSE provided by the Chief Executive Officer, Whitehorse



Whitehorse City Council
379-397 Whitehorse Road
Nunawading VIC 3131
Locked Bag 2 Nunawading VIC 3131

ABN: 39549568822

Telephone: (03) 9262 6333
Fax: (03) 9262 6308
TTY: (03) 9262 6325
TIS: 131 540

customer.service@whitehorse.vic.gov.au
www.whitehorse.vic.gov.au

4 September 2018

Enquiries: Ilias Kostopoulos
Telephone: 9262-6204
File Ref: 18/192581

Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31 / 35 Collins Street
MELBOURNE VIC 3000

Dear Mr Greaves,

Proposed Performance Audit Report – Security and privacy of surveillance technologies in public places

Thank you for your letter dated 22 August 2018 in relation to the proposed report on Security and privacy of surveillance technologies in public places.

Council officers have reviewed the report and acknowledge the gaps identified and recommendations suggested by VAGO. Council's approach to address the recommendations of the report is to initially establish an internal working group of key stakeholders across the organisation who have responsibility in this matter. The role of the working group will include a review of the Audit report recommendations and identify clear, agreed actions to address each of the recommendations.

The working group will also define appropriate and suitable timeframes by which each of the agreed actions will be undertaken. Our initial assessment of the report findings has determined that the delivery of particular actions will require funding by Council. Funding has not been included in Council's recurrent or capital works budgets for the 2018/2019 financial year to facilitate delivery of these actions. As such, Council will consider funding allocations in April 2019 during its Draft Council Budget considerations for the 2019/2020 financial year.

By this time, the working group will have had identified and established agreed actions that require funding and will have submitted new budget initiatives for Council's budget consideration. Council will consider and endorse the budget for 2019/2020 in June 2019. Given the assessment required by the working group and endorsement of next year's budget by Council, it is anticipated that the agreed actions will be delivered within the next 12 – 18 months.

In the interim, the working group will commence its review and updating of Council's CCTV policy and other procedures and process that need to be amended which do not necessarily require funding.

The VAGO report recommends that Council establish an agreement with the Victoria Police for the public safety CCTV system for the Box Hill Mall and laneways. We will raise this matter with the Victoria Police and seek to address it by December 2018. It is also our intention to take appropriate action to remove the relevant CCTV system hardware and monitor stored within the offices of the owner of the Box Hill shopping centre and have it relocated within secured Council property. This matter will be given high priority and an

RESPONSE provided by the Chief Executive Officer, Whitehorse—continued

investigation will commence in collaboration with the shopping centre owner to determine the scope of works and associated costs.

Should you have any further queries, please contact Ilias Kostopoulos, Manager Engineering and Environmental Services on 9262-6204.

Yours sincerely

A handwritten signature in dark ink, appearing to read 'Noeline Duff', with a stylized flourish at the end.

**Noeline Duff
CHIEF EXECUTIVE OFFICER
WHITEHORSE CITY COUNCIL**

RESPONSE provided by the Chief Executive Officer, Hume

Our File: HCC05/407 (IN2018/34688)
Enquiries: Gavan O'Keefe
Telephone: 9205 2240



1079 PASCOE VALE ROAD
BROADMEADOWS
VICTORIA 3047

Postal Address:
PO BOX 119
DALLAS 3047

Telephone: 03 9205 2200
Facsimile: 03 9309 0109
www.hume.vic.gov.au

Tuesday, 4 September 2018

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31 / 35 Collins Street
MELBOURNE VIC 3000

Dear Mr ~~Greaves~~ *Andrew*,

**RE: PROPOSED REPORT - SECURITY AND PRIVACY OF SURVEILLANCE
TECHNOLOGIES IN PUBLIC PLACES (YOUR REF 33503)**

I thank you for forwarding the Proposed Draft Report – Security and Privacy of Surveillance Technologies in Public Places, and offering the opportunity to provide submissions and comments to be included in the report.

Council has no disagreement with the general content and recommendations within the report. I would, however, like to make some comment on Hume's management of CCTV camera systems in the context of the report.

Hume City Council has acknowledged that surveillance technologies used in public places need policy direction, oversight and review. This is evidenced by the Council adoption of Council's CCTV Policy in late 2017, and my subsequent approval of the organisations Standard Operating Procedures.

The formal adoption of a policy is the first step of its implementation within an organisation. Hume City Council, as an organisation, has a clear and articulated approach to effecting its CCTV Policy, these are:

1. Formal Policy adoption
2. Development of Standard Operating Procedures to support/implement the Policy.
3. Circulation to affected managers of the Policy and their obligations under the Policy and Standard Operating Procedures.
4. Audit of existing CCTV cameras for compliance against the Policy.
5. Assessment of proposed sites for CCTV cameras against the Policy.
6. Upgrade, removal, installation of cameras, systems, signage etc. as recommended in the Audit and Assessment in 4 and 5 above, subject to budget/capital works approval.
7. Provide organisational (targeted training) education on the Policy and Standard Operating Procedures. Emphasis being on data (image) security and restricted access.

RESPONSE provided by the Chief Executive Officer, Hume—continued

2

8. Compliance checking that the managers and delegated staff are:
 - a. complying with the policy and standard operating procedures
 - b. have developed local procedures to ensure data management security in accordance with the Policy and Standard Operating Procedures.
9. Review of the Policy and Standard Operating Procedures for currency and incorporate amendments into the Policy and Procedures with lessons learned. This may be carried out by Council's internal auditors or precede such an internal audit.

Council is clear in its understanding that it has completed stages 1 – 6 and firmly plans to carry out stages 7 – 9. Council had always planned to carry out these last three stages; this was planned prior to VAGO advising that the Audit was occurring. That stages 7 and 9 have not yet been carried out is a matter of timing rather than omission.

Council will now incorporate the recommendations of the report into its ongoing implementation (and review) of its CCTV Policy and Standard Operating Procedures. It is planned that this implementation and review will be completed within twelve months of the tabling of the report.

I also wish to make a general comment regarding the report. Council views CCTV camera data, access and management within the totality of its information management policies and processes; in particular in how Council manages all personal and sensitive data it holds regarding individuals.

Council will not develop separate processes specifically for CCTV data, it will rely on its existing policies and procedures for compliance with the Privacy and Data Protection Act 2014 viz. information technology security, risk assessments, complaints handling, request for access etc. Council will, upon review of these policies and procedures, in accordance with the recommendation within the report, reference their application to CCTV data collection and handing by Council.

I again thank you for the opportunity to make comment on the proposed report and would like to convey my thanks to your Performance Audit Team, in particular Mr Tony Brown the Senior Manager who lead the team and ensured a professional, respectful and effective engagement with Council Officers.

Yours sincerely



DOMENIC ISOLA
CHIEF EXECUTIVE OFFICER

RESPONSE provided by the Chief Executive Officer, East Gippsland

Contact: Steven Columbus, Governance and Compliance Coordinator
Telephone No: (03) 5153 9500
Email: feedback@egipps.vic.gov.au

5 September 2018

Corporate Centre
273 Main Street (PO Box 1618)
Bairnsdale Victoria 3875
Telephone: (03) 5153 9500
National Relay Service: 133 677
Residents' Info Line: 1300 555 886
Facsimile: (03) 5153 9576
Email: feedback@egipps.vic.gov.au
ABN 81 957 967 765

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31/35 Collins Street
Melbourne VIC 3000

Dear Mr Greaves

Re: Proposed Performance Audit Report - Security and privacy of surveillance technologies in public places

Thank you for the opportunity to provide submissions and comment with respect to the proposed performance audit report, *Security and privacy of surveillance technologies in public places* (the Report).

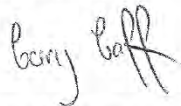
I have reviewed the Report and am comfortable that it represents the context fairly. I would also like to commend your officers on their approach. Council officers found them to be responsive and approachable throughout the lengthy audit process.

Council take its responsibilities with respect to the management of corporate and public safety CCTV systems very seriously. It is fair to say that governance and management processes have improved over time as the number and variety of surveillance technologies in public places have increased but as noted in your report, there remains considerable scope for improvement.

However, I contend that Council does have stringent work processes in place for the management of public CCTV systems in terms of acquisition, access, use and disclosure and information management, and these do not exist as mere window-dressing. With this in mind, I was pleased to note that Council's management and oversight of its recently implemented drone program came through the audit process very positively.

In accordance with section 16(3) of the *Audit Act* 1994, at **Attachment 1** to this letter I have taken this opportunity to respond to the nine formal recommendations included in the Report, together with implementation timelines for each.

Yours sincerely



GARY GAFFNEY
Chief Executive Officer

Website: www.eastgippsland.vic.gov.au Twitter: @egso Email: feedback@egipps.vic.gov.au



RESPONSE provided by the Chief Executive Officer, East Gippsland—continued

ATTACHMENT 1

Audit Recommendation	Council Response
<p>1. Review and update their CCTV policies to address the requirements of the <i>Privacy and Data Protection Act 2014</i></p>	<p>The minor additions recommended by VAGO at Figure 2A of the Report will be incorporated into the existing Public Space Closed Circuit Television (CCTV) Surveillance Policy and Code of Practice.</p> <p>In addition, the intent of Council is to develop a standalone policy/procedure for the management and oversight of corporate CCTV systems. This will ensure that Council's existing "robust control environment" (p52) is documented and communicated to staff appropriately.</p> <p>While relevant aspects are incorporated in the CCTV Code of Practice, the corporate CCTV system merits its own document, not least due to the privacy/surveillance implications of CCTV for employees of East Gippsland Shire Council. It will also provide the vehicle for addressing the gaps identified in the Report with respect to corporate CCTV systems</p> <p>Responsible Officer: Governance and Compliance Coordinator</p> <p>Response to be implemented by: February 2019</p>

RESPONSE provided by the Chief Executive Officer, East Gippsland—continued

Audit Recommendation	Council Response
<p>2. Assess all CCTV systems installed prior to the approval of a CCTV policy to ensure they comply with the policy</p>	<p>All public safety CCTV cameras became operational after the Public Space Closed Circuit Television (CCTV) Surveillance Policy and Code of Practice were adopted by Council. They comply with the policy and procedure.</p> <p>A small number of corporate cameras were installed prior to these documents coming into effect. In recent years a process of management consolidation has occurred, bringing all corporate CCTV cameras under the oversight of the Information and Communication Technology team. All cameras within the corporate system are now managed within the same "robust control environment" (p52).</p> <p>However, as stated with respect to recommendation 2, the drafting of a standalone corporate CCTV policy/procedure provides the vehicle for addressing the gaps identified in the Report with respect to these systems, as well as an opportunity to formally document and reinforce existing management practices and controls with staff.</p> <p>It will also provide a catalyst to review whether all cameras meet the standards contained therein. This may establish the need for system upgrades, including improved access controls, audit logging and where necessary camera replacement. The case for this will be determined and financed through the approved 2018/19 budget bid that enables a full review of the operation and management of the corporate CCTV systems.</p> <p>Responsible Officer: Manager Information Services</p> <p>Response to be implemented by: Stage 1 of the upgrade to be completed 30 June 2019 with focus on access control and security. Camera replacements/additions to be reviewed as possible budget bids for future years.</p>

RESPONSE provided by the Chief Executive Officer, East Gippsland—continued

Audit Recommendation	Council Response
<p>3. Assess the privacy impacts of proposals to install new or additional CCTV surveillance devices in public places</p>	<p>As your report acknowledges: "Only East Gippsland could demonstrate that decisions to install new CCTV cameras in public places are informed by consideration of privacy impacts" (p9, 23).</p> <p>Council will continue to apply existing processes to ensure the appropriate balance between privacy and operational priorities is maintained. The existing checklist will be reviewed in light of the Report and consideration given to applying it to all future proposals for CCTV investment. This would be done within the context of developing the standalone corporate CCTV policy/procedure.</p> <p>Responsible Officer: Governance and Compliance Coordinator</p> <p>Response to be implemented by: February 2019</p>
<p>4. Develop site-specific operating procedures for their corporate CCTV systems to reflect the requirements of the <i>Privacy and Data Protection Act 2014</i> and their policies</p>	<p>As your report acknowledges: "East Gippsland maintains central oversight and control of the operation of its corporate CCTV activities by limiting access to the systems to minimise the need for oversight. Very few sites allow for live monitoring. At all others, data is recorded on storage equipment which staff cannot access. The council's IT department is responsible for the day-to-day support and maintenance of CCTV systems and for extracting required footage from these systems."</p> <p>The previously mentioned corporate CCTV policy/procedure will provide the appropriate medium to address any site-specific considerations (most notably for those few sites that do still support live monitoring), as well as provide a concise, one-stop shop for more general operational circumstances that staff may encounter, such as how to deal with system outages and questions from the public and Victoria Police about use and access to the systems.</p> <p>Responsible Officer: Governance and Compliance Coordinator</p> <p>Response to be implemented by: February 2019</p>

RESPONSE provided by the Chief Executive Officer, East Gippsland—continued

Audit Recommendation	Council Response
<p>5. Allocate responsibility for overseeing the operation of CCTV systems to an appropriate senior manager and implement regular reporting on key aspects of CCTV system use</p>	<p>As your report acknowledges: “other than at Melbourne and East Gippsland, there was little, if any, routine central oversight of the management of these systems by council. This means that senior management and councillors may not have adequate assurance that their CCTV systems are managed appropriately.” (p28)</p> <p>You found a “robust control environment” and “strong controls” related to access management and disclosure of footage at East Gippsland Shire Council (p.52-53).</p> <p>You note that: “Melbourne and East Gippsland are the only councils to provide regular public reporting on the use and management of their CCTV systems. However, even these councils report only on public safety CCTV systems rather than all their CCTV systems.” (p9)</p> <p>As you assert, East Gippsland Shire Council has not previously undertaken regular reporting on key aspects of corporate CCTV system use. The form and frequency of such reporting will be considered as part of the development of Corporate CCTV policy/procedure</p> <p>Responsible Officer: Manager Administration Services</p> <p>Response to be implemented by: February 2019</p>
<p>6. Include a periodic audit of CCTV system use and data security in their forward internal audit programs</p>	<p>The East Gippsland Shire Council Internal Audit Plan 2018-2021 has recently been endorsed by the East Gippsland Shire Council Audit and Risk Committee.</p> <p>The possibility of the Internal Auditor undertaking an audit of CCTV system use and data security will be considered when the 2018-2021 Internal Audit Plan has its first annual review during 2018-2019.</p> <p>In addition, system use and data security will be audited by a Council officer on an annual basis with a report on that officer’s findings submitted to the Audit and Risk Committee for review.</p> <p>Responsible Officer: Governance and Compliance Coordinator</p> <p>Response to be implemented by: June 2019</p>
<p>7. Review and update the content and position of all signage in locations with corporate CCTV systems to reflect better practice</p>	<p>Council will review and update the content and position of all signage with respect to corporate CCTV systems in light of the considerations raised in the Report around content and positioning (p43-44).</p> <p>Responsible Officer: Manager Administration Services</p> <p>Response to be implemented by: 30 June 2019</p>

RESPONSE provided by the Chief Executive Officer, East Gippsland—continued

Audit Recommendation	Council Response
<p>8. Review and address access control and data security weaknesses for corporate CCTV systems</p>	<p>The CCTV upgrade scheduled for 2018/19 aims to centralise footage access, increase security of footage, provide greater visibility for footage to assist with investigations and review functional improvements in both the cameras and supporting software. Security of DVRs will also be addressed through the project.</p> <p>Responsible Officer: Manager Information Services</p> <p>Response to be implemented by: Upgrades to be completed 30 December 2019 with focus on access control and security.</p>
<p>9. Ensure regular audits and evaluations of public safety CCTV systems and hold the oversight committees for these systems to account for meeting their responsibilities under agreements with Victoria Police.</p>	<p>As detailed at p62 of the Report, East Gippsland Shire Council has a public-space CCTV Steering Committee in place that oversees and makes public an Annual Review of the program that “provide[s] relevant and useful information on the operation of the system, including its impact on perceptions of public safety and analysis of local crime data” and includes “a section on compliance, with agreed operating and use requirements”.</p> <p>Council takes no other “regular steps to monitor whether Victoria Police has met its appropriate use and data security obligations”.</p> <p>Informal visits by Council officers to the police station to assess whether the system is working and being used as intended ceased in July 2017, as a result of increasing workload in the governance area and competing priorities.</p> <p>At the point of next service contract negotiation, provision for the extraction of relevant information from the user activity audit logs available from the system will be taken up with ATR. The information sourced from the system can then then be reviewed against the manual log of user activity maintained by Victoria Police.</p> <p>Responsible Officers: Manager Administration Services / Manager Information Services</p> <p>Response to be implemented by: Will form part of contractual discussions in December 2019</p>

RESPONSE provided by the Chief Executive Officer, Horsham



Our Reference: :SB:fk

4 September 2018

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31, 35 Collins St
Melbourne 3000

Dear Mr Greaves

Audit - Security and privacy of surveillance technologies in public places

Thank you for providing the opportunity to respond to the recommendations directed to Horsham Rural City Council in your audit into security and privacy of surveillance systems in public places.

Council welcomes the audit to assist it in keeping pace with public expectations of accountability and privacy protection in this developing area.

While noting that there are ten recommendations of relevance to Horsham Council in this regard, I also wish to take this opportunity to re-state that Council has had no issues of privacy concerns or security breaches raised with it regarding its CCTV systems. This point is reflected within your report, which also notes that the Office of the Victorian Information Commissioner has reported no such breaches in Victoria.

Notwithstanding this, Council accepts the related premise of the report, i.e. that Council should be able to demonstrate that it is securely maintaining these systems to avoid any such breach.

I have attached to this letter a summary table that provides a response on Council's planned actions for each recommendation, including a proposed timeframe for each action. I wish to point out that some initial work is required to fully scope out the actions required for some of the recommendations. For these recommendations the table lists a timeframe for an interim response, by which time Council will have fully scoped out the required actions and the timeframe for those.

Please contact either John Martin, Director Infrastructure (5382 9724), or me if you have any questions about this response.

I would appreciate being advised of the intended timing of the report being tabled in Parliament.

Yours faithfully

SUNIL BHALLA
Chief Executive Officer

Address correspondence to: Chief Executive Officer PO Box 511 Horsham Victoria 3402
Civic Centre 18 Roberts Avenue Horsham Victoria 3400
Ph 03 5382 9777 Fax 03 5382 1111 Email council@hrcc.vic.gov.au Website: www.hrcc.vic.gov.au

RESPONSE provided by the Chief Executive Officer, Horsham—continued



Attachment

VAGO Audit - Security and privacy of surveillance technologies in public places

**Response to Recommendations
Horsham Rural City Council**

Recommendation	Proposed Action	Proposed Timeframe
1. Review and update their CCTV policies to address the requirements of the Privacy and Data Protection Act 2014	To be done in conjunction with recommendation 10, below.	By 31 December 2018
2. Assess all CCTV systems installed prior to the approval of a CCTV policy to ensure they comply with the policy	Assessment to be conducted after adoption of Policy as per recommendations 1 and 10.	31 March 2019 for assessment. Timeframe for subsequent actions to be determined.
3. Assess the privacy impacts of proposals to install new or additional CCTV surveillance devices in public places	No new CCTV installations until adoption of the Policy. All new proposals to be reviewed based on process outlined in Policy (or related procedure).	Ongoing, following implementation of Policy.
4. Develop site-specific operating procedures for their corporate CCTV systems to reflect the requirements of the Privacy and Data Protection Act 2014 and their policies	Assessment to be conducted after adoption of Policy as per recommendations 1 and 10.	31 March 2019 for assessment. Timeframe for subsequent actions to be determined.
5. Allocate responsibility for overseeing the operation of CCTV systems to an appropriate senior manager and implement regular reporting on key aspects of CCTV system use	This will be overseen by the Manager Governance and Information Management.	Responsibility confirmed at executive meeting on 4 September 2018
6. Include a periodic audit of CCTV system use and data security in their forward internal audit programs	Programming of this action to be included in internal audit schedule asap, with details to be based on the Policy and Agreement with Victoria Police	31 October 2018 for initial programming. To be confirmed after adoption of Policy.
7. Review and update the content and position of all signage in locations with corporate CCTV systems to reflect better practice	Review of existing signage Installation of additional signage as required	31 October 2018 31 December 2018
8. Review and address access control and data security weaknesses for corporate CCTV systems	Conduct review to determine issues Subsequent actions	31 December 2018 Dependent on outcomes of assessment
9. Ensure regular audits and evaluations of public safety CCTV systems and hold the oversight committees for these systems to account for meeting their responsibilities under agreements with Victoria Police.	As per recommendation 6	
10. Establish and implement a policy to cover all council CCTV systems.	Existing draft policy to be updated and adopted.	31 December 2018

Address correspondence to: Chief Executive Officer PO Box 511 Horsham Victoria 3402
Civic Centre 18 Roberts Avenue Horsham Victoria 3400
Ph 03 5382 9777 Fax 03 5382 1111 Email council@hrcc.vic.gov.au Website: www.hrcc.vic.gov.au

Appendix B

Arrangements with Victoria Police for public safety CCTV systems

Figure B1

Assessment of council arrangements with Victoria Police for public safety CCTV systems

Council	Assessment	Observations and issues
Melbourne	✓	<ul style="list-style-type: none"> Melbourne's public safety CCTV system, known as the Safe City Camera Program, began operating in February 1997. The current MoU with Victoria Police was signed in 2015. Melbourne is responsible for: <ul style="list-style-type: none"> continuous monitoring of public safety CCTV cameras providing Victoria Police with continuous live footage from these cameras providing targeted surveillance of public spaces when requested by Victoria Police notifying Victoria Police of certain types of incidents that are identified during the monitoring of public safety CCTV cameras. While Victoria Police receives live footage, the MoU does not allow it to record or copy the images. Melbourne provides copies on request, and Victoria Police is responsible for the storage and destruction of copies of recordings provided, in accordance with Victoria Police policies and procedures. Melbourne established an audit committee to oversee the public safety CCTV system operations by: <ul style="list-style-type: none"> providing an independent review and checking mechanism to ensure the public safety CCTV system meets its operating procedures and protocols promoting public confidence in the public safety CCTV system by ensuring its operations are transparent to the public and under ongoing independent scrutiny and review recommending actions that will safeguard the public safety CCTV system against any abuse. The committee: <ul style="list-style-type: none"> comprises a community representative and other independent members with relevant expertise, who devote significant time and effort to support the committee meets regularly—it met eight times between January 2017 and June 2018 discusses a wide range of matters, including data security and privacy issues, associated with the use of the system has regularly sought advice and assurances from Victoria Police about its management of public safety CCTV footage provided by the council.

Figure B1

Assessment of council arrangements with Victoria Police for public safety CCTV systems—*continued*

Council	Assessment	Observations and issues
Melbourne	✓	<ul style="list-style-type: none"> The audit committee provides the council with an annual audit report on the system, which is made public. This report provides information on the operations of the public safety CCTV system for a calendar year and seeks to evaluate whether the system complies with operating procedures. The findings and conclusions in the report are communicated in the language of a limited or negative assurance review rather than an audit or reasonable assurance engagement. For example, findings include that the audit committee found no evidence of failure by program staff to observe security protocols and standard operating procedures and no evidence of access to the control room outside the scope of the standard operating procedures and security protocols. While the report covers access controls for the public safety CCTV system control room and deals with controls for the provision of information, it does not specifically examine the strength or operation of IT security controls for public safety CCTV system information. Melbourne commissioned a review of the Safe City Camera Program in 2012. This review examined the terms of reference and operation of the audit committee and its annual audit process. The report resulting from this review was finalised in June 2013 and included a number of suggested changes and recommendations directly addressing key audit committee functions. The review suggested that an internal audit be scheduled every three years on the management of data security for the Safe City Camera Program. The council did not implement this suggestion, and the report was not provided to the audit committee for consideration. The manager of the Safe City Camera Program regularly meets with Victoria Police to discuss operational issues, and we saw clear evidence of close cooperation between the parties.
Whitehorse	X	<ul style="list-style-type: none"> Whitehorse has MoUs with Victoria Police for the public safety CCTV systems located in the Box Hill Gardens and at the Britannia Mall and adjacent council carpark in Mitcham. Whitehorse does not have an MoU with Victoria Police for the public safety CCTV system located in the Box Hill mall and laneways. The council advised that when this system was initially installed in 2011, the data was only stored on council equipment located in the Box Hill shopping centre security office. The council had an agreement with the owner of the shopping centre, and Victoria Police had to seek copies of CCTV footage from this company. The council's recording equipment and a monitor showing footage from this system are still located adjacent to the security control room in the Box Hill shopping centre. While the Box Hill mall and laneways CCTV system was installed in 2011, its management and use was not overseen by a steering committee until June 2014, when the council established a steering committee to oversee the Box Hill Gardens public safety CCTV system. This committee also oversees the Box Hill mall and laneways system. Whitehorse has not formally evaluated the operation or effectiveness of its CCTV systems. Whitehorse could not demonstrate that it has monitored whether Victoria Police has met its appropriate use and data security obligations and documented all images and footage copies taken from the systems.

Figure B1

Assessment of council arrangements with Victoria Police for public safety CCTV systems—*continued*

Council	Assessment	Observations and issues
Whitehorse	X	<ul style="list-style-type: none"> Our review of the minutes of the two steering committees overseeing the public safety CCTV systems at Britannia Mall and the Box Hill sites found that: <ul style="list-style-type: none"> they have each met once annually since 2014 both committees include representatives from the council and Victoria Police—the committee overseeing the Box Hill systems includes a representative from the owner of the Box Hill shopping centre, but neither committee includes members from the community or local traders, despite the MoUs indicating they should include other invited stakeholders they have not discussed privacy and data security issues these committees do not receive written reports from the council or Victoria Police to support their work—instead, their meetings typically involve verbal updates and focus largely on operational and maintenance issues and how effective the systems are in supporting Victoria Police both committees have failed to develop the monitoring and evaluation framework required for each system—the minutes of committee meetings record very high-level discussion around the use and effectiveness of the systems but no systematic framework and approach. Whitehorse sought to meet its MoU obligations to establish an audit committee for each of the Box Hill Gardens and Britannia Mall systems by assigning this role to the council's audit and risk committee. The council's CCTV policy further delegates this role to the council's risk management committee which comprises: <ul style="list-style-type: none"> the council's executive management team the manager, compliance the risk and insurance coordinator. Minutes from the steering committees are provided to the council's risk management committee. However, there is little evidence that this committee has actively discharged its role to uphold the integrity of the public safety CCTV systems and no evidence that it has reported to the council's audit and risk committee on how it is performing its responsibilities for overseeing both public safety and corporate CCTV systems. Further, the risk management committee has not identified the failure of the steering committees to develop a monitoring and evaluation framework for each system.
Hume	X	<ul style="list-style-type: none"> Hume has an MoU with Victoria Police for the Sunbury Town Centre public safety CCTV system. The steering committee was formed in 2014 and: <ul style="list-style-type: none"> includes representatives from the council, Victoria Police and local businesses meets regularly and has a primary focus on operational and maintenance activities and issues, with no substantive coverage or questions about information privacy or data security has discussed logging and reporting the frequency of Victoria Police viewing and copying footage from the system. Despite advising the former Department of Justice in August 2014 that it was forming the audit committee required by the MoU at that time, Hume did not establish this committee until June 2017. The audit committee agreed in June 2017 to conduct six-monthly compliance audits at the Sunbury Police Station. However, no audits had been undertaken by July 2018.

Figure B1

Assessment of council arrangements with Victoria Police for public safety CCTV systems—*continued*

Council	Assessment	Observations and issues
Hume	X	<ul style="list-style-type: none"> Hume's <i>Community Safety Action Plan 2015–2019</i> included a commitment to an annual audit and evaluation of the Sunbury Town Centre public safety CCTV system. The council assigned responsibility for this to the steering committee and the audit committee. Hume has not met this public commitment to annual audits and evaluations. Hume evaluated the system's impact on perceptions of public safety in 2015 but has not undertaken any recent evaluations. Hume could not demonstrate that it has monitored whether Victoria Police has met its appropriate use and data security obligations and documented all images and footage copies taken from the system.
East Gippsland	Partly met	<ul style="list-style-type: none"> East Gippsland has an MoU and a code of practice with Victoria Police for the public safety CCTV system that covers areas in the central business districts of Bairnsdale and Lakes Entrance. The MoU was first signed in 2014 when the system was established, and it was updated in June 2018 to reflect additional cameras. The steering committee was established in 2014 and: <ul style="list-style-type: none"> includes representatives from the council, Victoria Police and local businesses who provide an overview of relevant issues since the previous annual meeting meets annually oversees an annual review of the system which examines its effectiveness and assesses compliance with the operating procedures and safeguards covers operational and maintenance activities and issues has included limited discussion on information privacy or data security has discussed the extent to which Victoria Police is comprehensively logging its use of the system. The council's audit committee performs the functions assigned to the audit committee required by the MoU. The annual reviews are made public and provide relevant and useful information on the operation of the system, including its impact on perceptions of public safety and analysis of local crime data. The annual reviews include a section on compliance, with agreed operating and use requirements. In 2017, the steering committee changed its description of the process undertaken to support these findings from <i>audit</i> to <i>assessment</i>, to better reflect the extent of the review. The compliance section in both the 2016 and 2017 annual reviews were based on advice from Victoria Police, and the council did not test the information provided. There was also little explicit coverage of the management of privacy and data security risks other than references to secure locations for CCTV servers and monitoring equipment, and the secure destruction of data. Notwithstanding this, the 2017 annual review stated that the steering committee is 'confident that the Public Space CCTV program meets all the requirements of the PDPA and the <i>Surveillance Devices Act 1999</i>'. The 2017 review included the Victoria Police register of usage of the CCTV system for the 2017 calendar year but noted challenges in ensuring all use of the system is documented. Minutes from the steering committee meeting in October 2017 indicate that Victoria Police is not confident that every use of the system is recorded by its members. Council management informed the audit committee in November 2017 that installation and operation of the public safety CCTV program generally complied with requirements.

Figure B1

Assessment of council arrangements with Victoria Police for public safety CCTV systems—*continued*

Council	Assessment	Observations and issues
East Gippsland	Partly met	<ul style="list-style-type: none"> East Gippsland could not demonstrate that it takes any other regular steps to monitor whether Victoria Police has met its appropriate use and data security obligations and documented all images and footage copies taken from the system. The council advised that visits to the police station to assess whether the system is working and being used as intended ceased around July 2017, when the council officer who had overseen installation of the system left the council.
Horsham	X	<ul style="list-style-type: none"> Horsham has an MoU and a communication and liaison protocol with Victoria Police for the Horsham Town Centre public safety CCTV system. The MoU was first signed in 2014, and it was updated in June 2017 to reflect additional cameras. The steering committee was established in 2014 and: <ul style="list-style-type: none"> has met on four occasions, but not since 2015 includes representatives from the council and Victoria Police but none from local businesses or the community focuses largely on operational and maintenance activities and issues with little, if any, discussion on information privacy or data security issues. Horsham has not established the audit committee required by the MoU and has not audited use of the system. In 2014, the council and Victoria Police committed to regular audits to ensure that management and use of the system is accountable and fully complies with relevant requirements, to provide assurance to the public that the camera network is operated transparently and ethically. In 2014, the council and Victoria Police also committed to regular evaluations of the CCTV system to establish whether it complied with its original purposes and had achieved its objectives. The council has provided required reports to the state government to acquit grants for the system but has not completed the promised evaluations of compliance and effectiveness.

Source: VAGO based on review of council information.

Appendix C

Site pictures of CCTV signage and equipment

Figure C1
Good CCTV signage at council sites



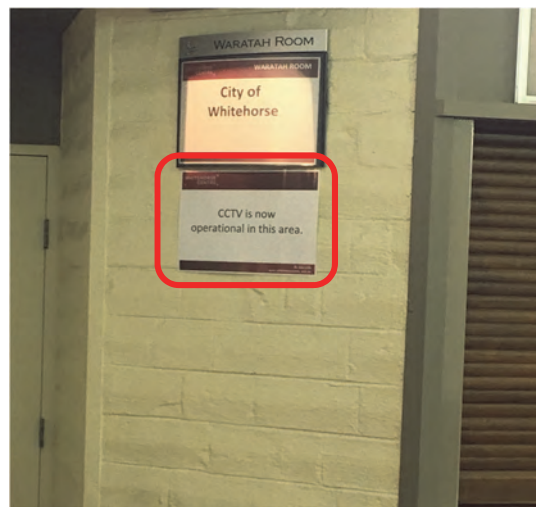
CCTV signage inside a council building.



CCTV signage at the gate of a 'Transfer Centre'.



CCTV signage at the entrance to a council's Art Centre Building.



CCTV signage inside the premises of a council's Arts Centre.

Figure C2

Council CCTV equipment in poor physical security and environmental conditions



Public safety CCTV system Network Video Recorder equipment kept in an unlocked rack located in an open staff work area.



Public safety CCTV rack unlocked and hosted in the maintenance room for a public toilet, without any temperature, humidity or water detection controls.



Digital Video Recorder for a CCTV system kept insecurely on the top of an office locker shelf.



Digital Video Recorder kept inside an unlocked wooden cabinet without any environmental controls.

Appendix D

Detailed findings on use, disclosure and access

Melbourne

Melbourne's policy for its public safety CCTV system guides the system's use, including disclosure of footage and access:

- Victoria Police can apply to view and obtain a copy of electronic media. Members of the public (or their legal representatives) may also make an application but must have a criminal or civil matter pending before they can view or request a copy of electronic media.
- The council encourages police to view footage before applying for a copy of the data. To view footage, police members must complete a written request and have it authorised. A similar process applies to the release of footage.
- Melbourne allows some flexibility around the application of these controls in emergency situations. Victoria Police can also view live footage from the public safety CCTV system cameras at various Victoria Police facilities.
- Melbourne follows a similarly tightly controlled process when dealing with requests from individuals and other third parties seeking access to or copies of footage from the public safety CCTV system.

Melbourne's policy for corporate CCTV systems indicates that:

Distribution of footage to external organisations will only be to law enforcement officers or integrity bodies, or organisations empowered by law to request information. Members of the general public will need to go through the legal process to obtain footage provided to external organisations, or they may apply through the *Freedom of Information Act 1982* process to Melbourne. Each copy produced will be recorded in a register which will also be used to document the distribution of recorded footage.

Melbourne maintains an incident management system for both the public safety CCTV system and corporate CCTV systems. It documents details of requests for access to footage and the outcomes from these requests. Melbourne keeps a master copy of all public safety CCTV system footage released to Victoria Police and others, but does not retain copies of footage from its corporate CCTV systems provided to external parties including Victoria Police.

We are satisfied that Melbourne maintains adequate controls for the release of CCTV footage to Victoria Police and other third parties and individuals.

Whitehorse

Whitehorse's CCTV policy includes information for the media and general public on requests for access to CCTV footage from both the public safety and corporate CCTV systems. The policy refers requests relating to the public safety systems to Victoria Police and indicates that freedom of information requests for access to corporate CCTV footage will be managed using the council's standard processes.

Whitehorse does not maintain a single comprehensive register of corporate CCTV footage provided to Victoria Police or other third parties. Most requests come from Victoria Police, and these are handled by the managers of the relevant sites. Managers review and save relevant CCTV footage and provide copies of still images and footage to Victoria Police on request. This is appropriate, but we suggest that Whitehorse keep a register of all such material provided to Victoria Police from all sites to fully comply with Information Privacy Principle 2.

We also saw an example where a parent requested CCTV footage from the Box Hill AquaLink site for an incident involving their child. Whitehorse released the footage after taking reasonable steps to:

- verify the legal status of the parent
- redact identifying information concerning other individuals in the footage
- specify terms and conditions for how the footage could be used.

Hume

Hume's CCTV policy indicates that:

- CCTV data is not collected for the purposes of public access and disclosure
- any request for access to CCTV data by external parties, other than an enforcement agency, shall be made in accordance with the *Freedom of Information Act 1982* and with council's request process.

Hume reported an increase in the number of requests from individuals for access to corporate CCTV footage. It deals with these requests as freedom of information requests.

Hume keeps a central register of video footage extracted from corporate CCTV systems in response to requests from Victoria Police and for other purposes. We cannot be assured about the completeness of the register as there is no reconciliation process between user activity audit trails in corporate CCTV systems and the register.

East Gippsland

Under East Gippsland's CCTV policy, the Director, Corporate, or the Victoria Police Manager reviews and/or approves written applications to use or view recorded information, depending on whether the relevant information is held by the council or Victoria Police.

The council has advised staff that it will not release footage to private citizens but will accept requests in writing from Victoria Police. If individuals seek access to CCTV footage in relation to motor vehicle accidents or potential criminal activity such as theft or assault, the council advises them to ask Victoria Police to request access to the footage from the council. The council then processes these requests.

The council's processes authorise only two designated IT staff to extract copies of footage from corporate CCTV systems, and it keeps a register showing footage extracted from these systems in response to requests from council staff and the police. This provides a robust control environment.

Horsham

Horsham's lack of an approved policy for its CCTV systems and activities means that there is no clear, easily accessible information available to the public on how to request access to footage.

There is also little documented information available to local facility managers on how to deal with requests from Victoria Police, the public and the media to access CCTV footage.

Horsham does not keep a register of corporate CCTV footage viewed or copied and released to Victoria Police and other external parties. This material is stored on a single laptop which creates other risks.

Auditor-General's reports tabled during 2018–19

Report title	Date tabled
Local Government Insurance Risks (2018–19:1)	July 2018
Managing the Municipal and Industrial Landfill Levy (2018–19:2)	July 2018
School Councils in Government Schools (2018–19:3)	July 2018
Managing Rehabilitation Services in Youth Detention (2018–19:4)	August 2018
Police Management of Property and Exhibits (2018–19:5)	September 2018
Crime Data (2018–19:6)	September 2018
Follow up of Oversight and Accountability of Committees of Management (2018–19:7)	September 2018
Delivering Local Government Services (2018–19:8)	September 2018

All reports are available for download in PDF and HTML format on our website
www.audit.vic.gov.au

Victorian Auditor-General's Office
Level 31, 35 Collins Street
Melbourne Vic 3000
AUSTRALIA

Phone +61 3 8601 7000
Email enquiries@audit.vic.gov.au