District of Barriere

REPORT TO COUNCIL
Request for Decision

Date: July 15, 2024	**File:** 530.20/Rpts
To: Council	**From:** Chief Administrative Officer
Re: Video Surveillance on District-owned Property Policy No. PS48	
Recommendation: ***That Video Surveillance on District-owned Properties Policy No. PS48 be adopted as presented.***	

Purpose

To introduce a policy on Video Surveillance on District-owned Property to Council for feedback, discussion, and potential adoption.

Background

At the Regular Meeting of Council on June 24, 2024, Staff presented an update on potential options to increase security efforts at the Bandshell location in Fadear Park. (For reference, the memorandum is attached for convenience).

In the past, Staff has already tried to educate the public with various signage to deter theft; however, break-in attempts have continued over the years, and with expensive equipment being located now at Fadear Park (and other critical infrastructure being located for example at Well sites) it is reasonable for Council to review other methods to ensure that security for District assets, Staff, and the public are increased.

The Barriere Business Center (BBC) is also a District-owned building, and plans are in place as well to install some video surveillance systems. As such, it would be beneficial to have guidelines created that meet or exceed legislated recommendations.

Policy

As previously indicated, a Policy will be required to meet guidelines from the Office of the Information and Privacy Commissioner (OIPC).

The purpose of the Policy (see attached DRAFT Policy) is to set guidelines for the implementation of any Video Surveillance in District-owned or occupied buildings or outdoor public spaces, and set the rules for governing access to, and disclosure of, stored video footage and images.

For example, the policy addresses the retention period for footage which would be set to a minimum of 7 days and a maximum of 21 days depending on available data storage or based on limitation from the surveillance equipment provider. Footage would be retained more than the normal retention period where the footage is required as part of an investigation, or for the purposes of evidence.

Only select staff would have access to the recorded footage and only when investigating:

i. Mischief
ii. Criminal behavior
iii. Vandalism
iv. Harm to another individual
v. Theft, including theft from vehicles
vi. Other such nuisances that the District finds necessary to investigate
vii. Other instances that may arise, but access to the data must first be approved by the CAO - unless life or safety is at risk, at which point it would be considered an emergency and emergency personnel (Fire, Police, Ambulance, or other) may request access.
viii. A personal injury accident

The Policy also includes guidance to tenants of District-owned facilities such as the BBC.

Various operational exclusions have been added that as well would for example allow monitoring of wastewater equipment or allow video recording for training purposes, for example for the fire department.

Benefits or Impact

General
Implementing this Policy will allow staff to install video surveillance equipment that is intended to protect the health and safety of our staff, volunteers, and the public. In addition, this could support other partners with their endeavors for the safety and security of their patrons in District-owned facilities.

Finances
At this time, no additional funding is required to implement basic video surveillance options. If deemed necessary in the future, Staff would present to Council at annual budget meetings any significant planned capital expenses to increase the quality of equipment used.

Strategic Impact
Crime Prevention and Enhance Public Safety

Risk Assessment
Compliance: OIPC guidelines for Video Surveillance and established regulations
Risk Impact: Low

Internal Control Process: Staff are following OIPC guidelines and have worked with other municipalities and HR related templates to ensure the risk remains low and privacy guidelines are followed.

Next Steps / Communication

- If approved, complete Privacy Impact Assessment (PIA)
- Procurement of basic video surveillance equipment and installation
- Installation of signage where required
- Work with tenants of District-owned facilities regarding potential video surveillance options

---

Attachments

- Policy No. PS48 – Video Surveillance on District-owned Properties – DRAFT
- OIPC of BC guidance document for Video Surveillance
- Previously Received Memorandum from the June 24, 2024, Regular Meeting of Council

---

Recommendation:
That Video Surveillance on District-owned Properties Policy No. PS48 be adopted as presented.

Alternative Options

1. Council could amend the draft policy. Please note that any changes should be within the expectations from the OIPC and may require additional research before the Policy can be adopted.
2. Council could also determine not to proceed with any Policy at this time at this time and subsequently Staff would not proceed with implementing any video surveillance measures.

Prepared by:
D. Drexler, Chief Administrative Officer

DISTRICT OF BARRIERE
COUNCIL POLICY MANUAL

Approval Date: DRAFT
Amended Date: N/A

NO: PS48
SECTION: Protective Services
SUBJECT: Video Surveillance on District-owned Property Policy

Purpose

The purpose of this policy is to set guidelines for the implementation of any Video Surveillance in District of Barriere (the 'District') owned or occupied buildings or outdoor public spaces and set the rules for governing access and disclosure of stored video footage and images.

Intent

The District is committed to the ongoing protection of the health and safety of our employees, volunteer fire fighters, volunteers, customers and visitors as well as the protection of property, both physical and intellectual. In pursuit of this commitment, this Video Surveillance on District-owned Property Policy has been adopted to ensure that appropriate Video Surveillance of District premises is performed where personal safety or property security matters warrant.

Definitions

In this policy,

"Video Surveillance" means Surveillance performed using a video or still picture camera designed to monitor and/or record activity.

Policy Statements:

Video Surveillance

The District has a legal right and obligation to protect individuals in or around its buildings and its assets and the right to use Video Surveillance for this purpose. Video Surveillance can be useful in deterring crime and nuisance in unsupervised areas where full-time live surveillance is an unreasonable expectation due to the risks involved to District staff, or where costs are prohibitive. It should be acknowledged that Video Surveillance can be construed as an unreasonable invasion of personal privacy and the installation of Video Surveillance equipment should only be considered once a Privacy Impact Assessment (PIA) has been complete. It should also be acknowledged that the deployment of Video Surveillance by the District is not intended to infringe on the guaranteed rights and freedoms of individuals in any way by monitoring personal activity in public spaces. The intended purpose is to safeguard District-owned assets and individuals who use those assets.

General Video Surveillance Guidelines

1. The Chief Administrative Officer (CAO) will develop any specific policies and procedures required that exceed this Policy.

2. When installing Video Surveillance, District staff will ensure that the cameras are located in areas that create minimal intrusion to personal privacy.

3. Where possible, sound is not to be recorded.

4. The District will not use Video Surveillance to monitor or measure productivity.

5. The District will provide notice that the area is under surveillance by posting visible signs.

6. Video Surveillance will only be reviewed if an event has taken place that requires the recordings to be reviewed.

7. To ensure the ongoing privacy of our staff and the public at large, the District will ensure that only authorized personnel shall be allowed to operate Video Surveillance equipment, and review recordings.

8. The District shall retain all Video Surveillance recordings for approximately 7-21 days (the "Retention Period") or as practical depending on surveillance equipment provider. The Retention Period should be directly related to the available storage space and recording quality. The system should be designed to fill the storage and then recycle the space through degradation and deletion to ensure that at a minimum approximately 7 days of recordings are available if required.

9. Footage will be retained more than the normal Retention Period where the footage is required as part of an investigation, or for the purposes of evidence.

Access to Video Surveillance Recordings

10. All recordings shall be stored securely.

11. All recordings created by means of Video Surveillance shall be the sole property of the District, and may not be taken, reproduced, or destroyed for any reason without prior express written permission.

12. Reasons to access recordings include such instances as:

    a. The need to identify individuals that have been involved with, or incidents that have resulted from:

        i. Mischief
        ii. Criminal behavior
        iii. Vandalism
        iv. Harm to another individual
        v. Theft, including theft from vehicles
        vi. Other such nuisances that the District finds necessary to investigate
        vii. Other instances that may arise, but access to the data must first be approved by the CAO - unless life or safety is at risk, at which point it would be considered an emergency and emergency personnel (Fire, Police, Ambulance, or other) may request access.
        viii. A personal injury accident

13. Except for requests by law enforcement agencies, individuals must submit a formal request to view recordings, and the request will be subject to approval by the CAO.

14. If any law enforcement agency requests access to the District Video Surveillance recordings, the District will act in accordance with the law, and provide the materials as necessary.

15. Requests for access to recordings shall be undertaken in compliance with the *Freedom of Information and Protection of Privacy Act* (FOIPPA) as amended or replaced from time to time.

16. All activities regarding access to recordings from outside of the organization and the non-automated disposal of recordings shall be documented. Only authorized personnel shall have access to the surveillance activities documentation.

17. Authorized personnel shall be the only parties eligible to delete recordings, and then only in accordance with this policy, and following the expiration of the Retention Period, notwithstanding the requirements for retention in the event of an investigation or for the purposes of evidence.

18. Where recordings are disposed of, they must be deleted or destroyed in such a manner as to ensure that they cannot be viewed or accessed by anyone.

Unauthorized Access and/or Disclosure (Privacy Breach)

19. Any District employee who witnesses the unauthorized disclosure of any surveillance recordings that are in violation of this Policy, and/or a potential privacy breach must report the incident to the CAO immediately.

20. The District will investigate all reported breaches of privacy, unauthorized viewings, or disclosures. Any breaches of this Policy may result in disciplinary action up to and including termination of employment.

Exclusions

This Policy is not applicable to any requirements imposed by another level of government on the RCMP (Royal Canadian Mounted Police) or other police services.

This Policy does not apply to videotaping or audio taping of District Council meetings or events.

This Policy does not apply to videotaping or audiotaping for operational purposes, such as, but not limited to:

- Operational live streams and recording, e.g. snowfall, roadways, wastewater treatment, water systems, etc.
- Live camera web streams
- Recordings for training purposes
- Door Entry Devices (Doorbell cameras, etc.) – if used, these devices would follow this Policy as outlined above; however, are excluded from Section 3. and are allowed to record audio for two-way communication if necessary.
- Other operational needs as deemed necessary from time to time by the CAO.

Other Organizations

Organizations that manage District-owned facilities, are allowed to install video surveillance equipment, as long as they follow this District Policy which outlines surveillance footage access and retention periods, and the organization posts appropriate signage to notify the public.

Resolutions and Amendments

MMM DD, YYYY – Council Policy No. PS48 Established

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

GUIDANCE DOCUMENT

USING OVERT VIDEO SURVEILLANCE

OCTOBER 2017

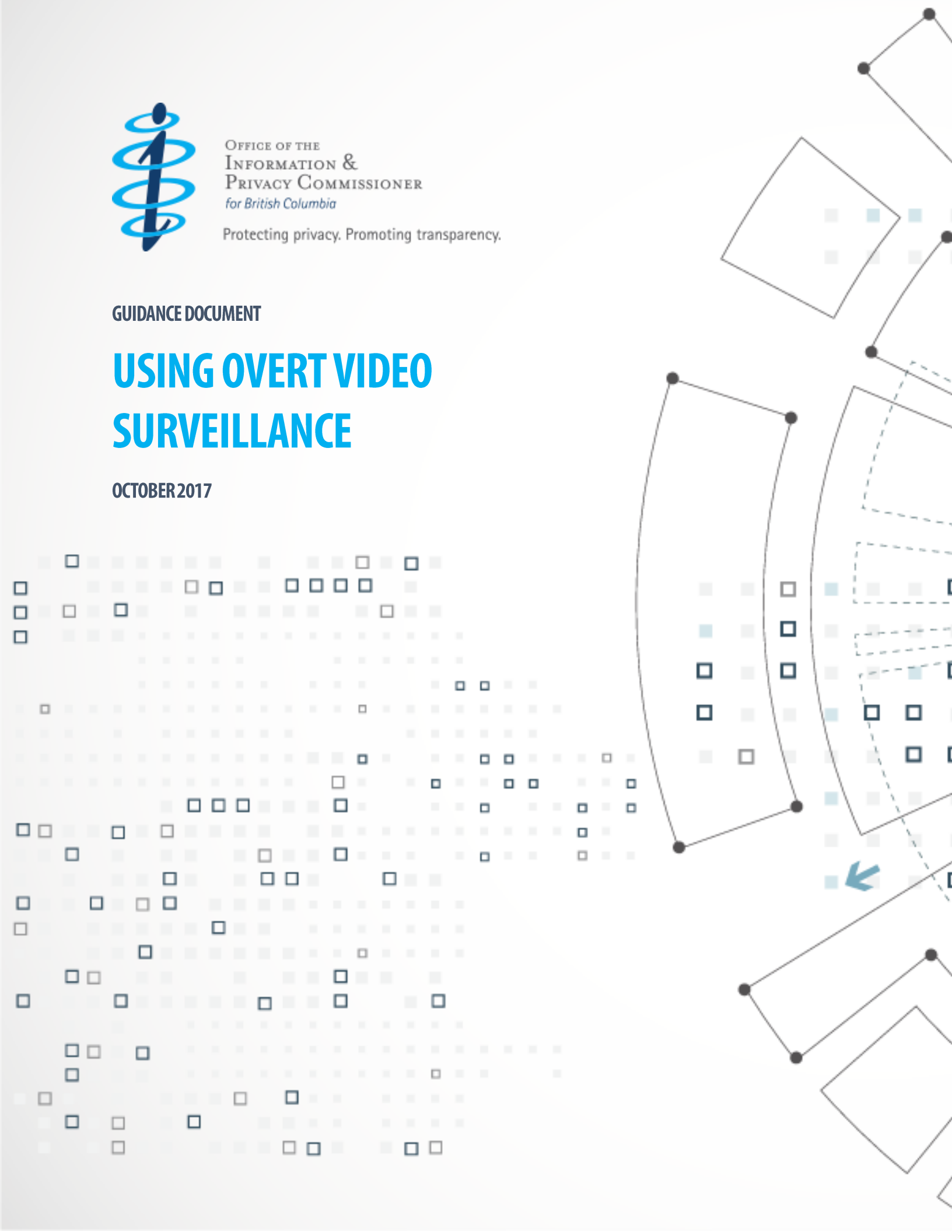

TABLE OF CONTENTS

PURPOSE OF THIS GUIDANCE DOCUMENT

This guide is for public bodies and organizations that are interested in using video surveillance in compliance with BC's *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). It recommends privacy protective measures that should be considered prior to installation of video surveillance systems.

APPROPRIATE USE

Installing surveillance equipment may seem like a logical decision for your organization, but collection and use of personal information through video surveillance may violate BC privacy law and could lead to other costly liabilities.

Video surveillance should only be used as a last resort after exhausting less privacy-invasive alternatives, such as improved workplace supervision or implementation of theft-prevention controls. Organizations need to consider whether video surveillance will achieve the intended purpose and whether the concerns are serious enough to warrant implementing this highly invasive technology.

POLICIES AND PROCEDURES

If collecting personal information via video surveillance is necessary and authorized under the legislation, you will need to develop appropriate policies and procedures. Your video surveillance policy should explain the rationale and purpose of the surveillance; when and how monitoring and/or recording will be in effect; how recordings will be used; for how long they will be kept; how they will be securely deleted; and a process to follow if there is unauthorized access or disclosure.

ADVICE FROM THE COMMISSIONER	Develop a surveillance policy.

LIMITED COLLECTION

The most privacy protective approach is to limit the time your surveillance is active. This means only turning on the cameras for certain times of the day or night rather than 24 hours a day, so you only monitor or record during the times that meets your specific need. For instance, if you operate a retail store and have experienced break-ins after hours, only use your cameras when the store is closed so that you are not capturing images of employees and customers during business hours.

Another consequence of video surveillance is that cameras may capture images of people who are not the intended subjects. This would not be authorized under FIPPA or PIPA. To ensure your surveillance is lawful:

- Position cameras to capture the least amount of information that is needed. For example, a store security camera should not capture images of passersby on the street.
- Avoid areas where people have a heightened expectation of privacy, such as change rooms, washrooms, or into windows.

ADVICE FROM THE COMMISSIONER	Limit the time your surveillance is active.
	Avoid unintended subjects.

LIMITED ACCESS

Your video surveillance policy should identify individuals who are authorized to access the recordings. Authorized individuals should only review the recorded images to investigate a significant security or safety incident, such as criminal activity. Minimize the number of individuals who have access to the monitoring system or recordings, and ensure they have adequate ongoing privacy training so they are clear about their legal obligations.

Any disclosure of video surveillance recordings outside your organization should be limited to that authorized by the applicable privacy law, and be documented.

Anyone whose image is captured by your surveillance video has the right to access their own personal images, so you must be prepared to provide a copy of the relevant surveillance recording upon request. When disclosing recordings, use masking technology to ensure that identifying information about other individuals on the recording is not disclosed.

ADVICE FROM THE COMMISSIONER	
	Limit access to recorded images to authorized individuals.
	Consider right of access.

SECURE STORAGE AND DESTRUCTION

Surveillance equipment should be securely stored to prevent theft of personal information and protect your employees, guests, customers—and your organization—from the risks of a privacy breach. To reduce the possibility of loss and theft, do not remove video recording from your premises and follow a secure storage protocol.

Prepare a retention and destruction schedule to specify the length of time that surveillance records will be kept (we recommend a maximum of 7 days). Decide when and how records will be destroyed. Safely and securely destroy recorded images when they are no longer required for business purposes. Document the destruction in your logs.

ADVICE FROM THE COMMISSIONER	
	Store any recorded images in a secure location.
	Destroy recorded images when they are no longer needed.

ACCOUNTABILITY

Post a clear, understandable notice about the use of cameras that is visible before individuals enter the premises. Providing notification is respectful of their privacy, gives them the option not to enter, and is required by law. The sign must plainly indicate which areas are under video surveillance and for what purpose, for example: “This property is monitored by video surveillance for theft prevention.” It must also provide contact information of someone in your organization for individuals to contact if they have questions about the surveillance.

Consider making your written surveillance policy available to the public. Your customers will appreciate your transparency and gain a better understanding of the purposes of the surveillance and the security measures that are in place to protect their personal information. Finally, regularly review your policy to ensure that using video surveillance is still justifiable and needed for your original purpose.

ADVICE FROM THE COMMISSIONER	
	Use adequate signage to notify the public.
	Allow access to your surveillance policy.
	Periodically re-evaluate your need for video surveillance.

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

These guidelines are for information purposes only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia. These guidelines do not affect the powers, duties, or functions of the Information and Privacy Commissioner regarding any complaint, investigation, or other matter under FIPPA or PIPA.

PO Box 9038 Stn. Prov. Govt. Victoria BC V8W 9A4 | 250-387-5629 | Toll free in BC: 1-800-663-7867
info@oipc.bc.ca | oipc.bc.ca | @BCInfoPrivacy

District of Barriere

REPORT TO COUNCIL
Memorandum

Date: June 24, 2024	**File:** 530.20/Rpts
To: Council	**From:** Chief Administrative Officer and Public Works Manager
Re: Bandshell Security	

Purpose

To provide Council with an update and next steps on the bandshell security issue which was previously discussed at past Council meetings.

Background

Multiple break-in attempts have occurred at the Bandshell in the last few years. We now have valuable equipment stored inside and a video security or facility alarm system would be beneficial to provide some level of protection for the facility and the assets. (For reference, the Report to Council from the June 10, 2024, meeting is attached for information only.)

Update

After reviewing the site for potential security solutions, it was determined that the best and most cost-effective solution would be to install a video/picture-based solution. Although facility alarm systems can be useful, often theft still occurs and there is no clear evidence of what happened prolonging RCMP investigations that generally are not successful in retrieving the stolen items.

Video surveillance on the other hand provides an opportunity to visually see what occurred. In other municipalities, the RCMP has been successful with utilizing these types of images and videos to determine who was responsible for the theft and the courts have been able to prosecute based on this type of evidence.

To fully utilize such video surveillance devices, Council must establish a policy regarding the storage, use, and access of picture/video footage that meets or exceeds privacy legislation and complies with guidelines of the Office of the Information and Privacy Commissioner (OIPC) for BC.

Staff have already ordered video surveillance signage to notify the public of potential video surveillance presence on-site and deter any additional break-in attempts at this time.

Finances

No additional costs to the 2024 operational budget are anticipated as the device is estimated at less than $300-500 and the cost would be absorbed within the already approved budgets. Monthly subscription plans per device are maximum $15 per month, so $180 per year.

Next Steps
Given all of the above, and Councils desire to implement a reasonable security solution, Staff intends to proceed with the following next steps unless Council instructs Staff otherwise:

- Prepare a Video Surveillance Policy for Council consideration (anticipated to be brought to Council for the July 15, 2024, meeting.
- If approved, Staff would complete a Privacy Impact Assessment (PIA) thereafter to be in compliance with provincial legislation.
- If the Policy is approved, Staff would also procure and install a cost-effective camera solution with cellular technology for transmitting images and alerting Staff who in return can alert 9-1-1 depending on the severity of the issue.

At this time the alert process is not determined and will need to be adapted over time; however, the following has so far been discussed: alerts would be sent to on-call staff or Public Works Manager. Staff would then inform 9-1-1 based on the issue at hand.

Other Future Opportunities
If the Video Surveillance Security Policy is adopted by Council, Staff would review other high-risk areas to potentially install similar equipment to enhance the protection of key assets such as the Well sites and the Public Works storage area at the septage receiving site where multiple attempted break-ins have been reported and some theft has occurred in the past. Council would be updated as part of the highlight report on the identified locations and if surveillance equipment was installed.

Attachments

- Previously Received Report from the June 10, 2024, Regular Meeting of Council

Alternative Options

1. If Council would like Staff to install an Alarm System instead of proceeding with the Next Steps listed above, Council should pass a motion to that effect.
2. Council could also determine not to proceed with any security solution at this time and pass a motion to that effect.

Prepared by:
C. Matthews, Public Works Manager
D. Drexler, Chief Administrative Officer

District of Barriere

REPORT TO COUNCIL

Date: June 10, 2024	**File:** 530.20/Rpts
To: Council	**From:** C. Matthews, Public Works Manager
Re: Bandshell Security System	

Background:

Multiple break-in attempts have occurred at the Bandshell in the last few years. We now have valuable sound equipment stored inside and a proper security/alarm system is necessary.

Discussion:

Staff have received a quote to install and monitor an alarm system. The alarm company has also provided costs for an optional camera inside the bandshell, as well as other locations that have experienced vandalism. At a minimum, Staff recommend the installation of an alarm system at the Bandshell. The cost for the alarm system materials and installation is estimated at $2000 with the purchase of a 3-year monitoring agreement. Basic monitoring at this facility will cost $34.95 per month plus GST (see attached quotation).
Staff will be researching options for a budget-friendly security camera that could provide live feeds inside when motion is detected. As the security system was an unforeseen cost, the purchase and monthly monitoring of the alarm system could be funded by general surplus.

Recommendation: That Council approve the purchase and installation of an alarm system from Peace of Mind Security Systems Inc. for an amount not exceeding $2,000.00 plus taxes, including entering into a monthly monitoring agreement in the amount of $34.95/month for Bandshell security with the funds coming from General Surplus.

Prepared by: C. Matthews, Public Works Manager
Reviewed by: T. Buchanan, Acting CAO