The Corporation of the City of Fernie
501-3rd Avenue, Box 190, Fernie, B.C. V0B 1M0
(T) 250.423.6817 | (F) 250.423.3034 | (E) cityhall@fernie.ca | (W) www.fernie.ca

Policy Title: Video Surveillance System Policy

Department:	Corporate Administration Services		
Approval Date:	Click here to enter a date.	**Approved By:**	Choose an item.

PURPOSE OF POLICY

This policy is to establish the guidelines for the use of video surveillance equipment and records to enhance the security and safety of persons and properties in the Historic Downtown Core.

SUMMARY

The intent of the City of Fernie's Video Surveillance System in the Historic Downtown Core is to improve public safety and deter crime, such as vandalism, graffiti and public mischief. The use of a video surveillance system by the City of Fernie will be restricted to the purposes of law enforcement.

Video surveillance recordings may be provided by the City of Fernie to the RCMP for use in an investigation and as evidence in any civil proceedings.

SCOPE AND APPLICABILITY

This Policy applies to any video surveillance system owned or operated by or for the City of Fernie in the Historic Downtown Core that may collect personal information about identifiable individuals in any form. It does not apply to video surveillance conducted by law enforcement agencies engaged in lawful investigation or videotaping of City Council meetings.

POLICY STATEMENT

The City of Fernie recognizes that video surveillance technology has a high potential for impacting individual expectations to privacy and does not wish to impair personal privacy any more than is warranted to provide necessary and reasonable protection of property against vandalism, theft, damage and destruction. To minimize impacts on personal privacy, the use of video surveillance technology will be reserved for legitimate law enforcement purposes and will be consistent with the guidelines set out by the Office of the Information and Privacy Commissioner (OIPC).

1. DEFINITIONS

"*Act*" means the *Freedom of Information and Protection of Privacy Act (FOIPPA), R.S.B.C.*

1996 Ch. 165, as amended from time to time.

"*FOIPPA Coordinator*" means the person or persons named to this position by City of Fernie Freedom of Information Bylaw.

"*FOIPPA Head*" means the person or persons named to this position by City of Fernie Freedom of Information Bylaw.

"*Open public space*" means the grounds of any real property, or portions of real property, owned or subject to a right of occupation by the City of Fernie to which the public is ordinarily invited or permitted to be on, and includes, but is not necessarily limited to, City streets, boulevards and sidewalks in the Historic Downtown Core.

"*Personal information*" means recorded information about an identifiable individual.

"*Privacy Impact Assessment (PIA)"* means an assessment that is conducted to determine if an enactment, system, project or program meets the requirements of the *Act*. For the purposes of this policy, the PIA will be in the format of the "Video Surveillance Proposal, Privacy Impact Assessment and Approval Form" as attached to this policy as Appendix "A".

"*Record*" means any recorded information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a videotape, a machine-readable record, and any record that is capable of being produced from a machine-readable record.

"*Transitory records"* for the purpose of this policy, means records that are created to be used only for a limited period of time for the preparation of an ongoing or final record. In this case regarding video surveillance, all surveillance records which do not record an incident providing the basis for an RCMP investigation will be considered transitory.

"*Video surveillance system*" means a mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing or monitoring of individuals, assets and/or property.

2. GENERAL PRINCIPLES

2.1. The City of Fernie wishes to make use of video surveillance systems to provide evidence of illegal activities or public nuisances for the purpose of law enforcement.

2.2. Before implementing a surveillance system or expanding an existing video surveillance system, the reason for introducing or expanding the video surveillance is to be clearly articulated in writing and approved by Council.

2.3. Video surveillance systems will only be considered after other, less intrusive, security

methods have been considered and have been found to be unworkable. Video surveillance systems shall be used in conjunction with other security efforts and initiatives.

2.4. Video surveillance systems should only be used to address a real, pressing and substantial problem of sufficient importance to warrant overriding of personal privacy issues. Concrete evidence of the problem should be supplied prior to implementation of any video surveillance system.

3. PRIVACY CONSIDERATIONS

3.1. Video surveillance systems that record images of individuals collect personal information that must be protected in accordance with the *Act.*

3.2. Video surveillance should be restricted to times when incidents are most likely to occur.

3.3. Video surveillance systems must be clearly visible and marked by prominent signage.

4. NOTIFICATION / SIGNAGE

4.1. Areas in the Historic Downtown Core subject to surveillance will be identified to those in the area by way of signage.

4.2. Video Surveillance Signage should be clearly visible, identifying the use of video surveillance cameras in the area where they have been installed. Signage will state the following:

"*This area is monitored by video surveillance cameras. For further information, please contact the City of Fernie Freedom of Information & Protection of Privacy Head, 501-3rd Avenue or at 250.423.6817 Monday through Friday between 8am and 5pm."*

5. RESPONSIBILITIES

5.1. FOIPPA Head Responsibilities

5.1.1. The FOIPPA Head is responsible for the overall video surveillance program.

5.1.2. The FOIPPA Head is responsible for ensuring the establishment of procedures for the use of video surveillance equipment, including the random audit of such procedures, in accordance with this policy, including monitors and storage devices, at irregular intervals and the results of each review should be documented in detail and any concerns should be addressed promptly and effectively.

5.1.3. The FOIPPA Head responsible for the life cycle management of authorized video surveillance systems, including, but not limited to, specifications, installation, maintenance, replacement, disposal, and related requirements, including signage.

5.1.4. Assigning a person responsible for the day-to-day operation of the system in accordance with the policy, procedures and the OIPC Surveillance System Privacy Guidelines that may be issued from time-to-time.

5.2. FOIPPA Coordinator is responsible for:

5.2.1. Documenting the reason for implementation of a video surveillance system at the designated area.

5.2.2. Maintaining a record of the locations of the reception (video camera) equipment.

5.2.3. Maintaining a list of personnel who are authorized to access and operate the system(s).

5.2.4. Maintaining a record of the times when video surveillance will be in effect.

5.3. City Employees and Service Providers

5.3.1. City of Fernie employees and service providers shall review and comply with the policy in performing their duties and functions related to the operation of video surveillance systems. City of Fernie officers and employees may be subject to discipline if they knowingly or deliberately breach the policy.

5.3.2. Service providers having access to video surveillance information must be bonded and sign a confidentiality agreement, as attached to this policy as Appendix "B", limiting access to, copying and disclosure of personal information and requiring compliance with this Policy. Breach of the confidentiality agreement may lead to penalties up to and including contract termination.

6. INSTALLATATION AND PLACEMENT

6.1. Video surveillance will not be installed in locations where confidential or private activities or functions are routinely carried out (ie. in front of medical facilities).

6.2. Equipment for reviewing recorded images should be installed in an area where access is strictly controlled. Only designated personnel (identified under section 5. Responsibilities) will normally have access to the access area and to the equipment.

6.3. Installation of video recording equipment should be restricted to areas identified as high crime or public nuisance areas in the Historic Downtown Core.

6.4. Cameras should not be directed to look through the windows of adjacent buildings.

6.5. Covert surveillance (ie. hidden cameras without signage) is not contemplated under this Policy.

7. ACCESS, USE AND DISCLOSURE

7.1. Access to video surveillance information is limited to the following individuals:

- Chief Administrative Officer
- FOIPPA Head
- City of Fernie Solicitor
- RCMP in relation to a law enforcement matter
- An Agent appointed by the City of Fernie

7.2. Only authorized personnel will monitor surveillance applications.

7.3. Video surveillance equipment shall only record data between the hours of 6:00pm to 8:00am daily.

7.4. Any records (videotapes, still photographs, digital images, etc.) produced by surveillance systems shall be kept in a secure, locked facility and managed appropriately to protect legal obligations and evidentiary values.

7.5. Access to the storage devices should be possible only by authorized personnel and access logs must be kept of all instances of access to, and use of recorded material.

7.6. Use of video surveillance data is to be for the purposes of investigation of incident(s) as required by the RCMP only, as described under section 2. General Principles.

7.7. Video surveillance monitors must be located so that the public is not able to see any video reproduction.

7.8. Only authorized personnel will view information and only where there is a need to do so as requested by the RCMP in relation to an investigation into an alleged crime, either because an incident has been reported or is suspected to have occurred.

7.9. Information Technology service providers will access the equipment only for the purpose of maintaining, backing up the software, and assisting with the extraction of the portions of the data.

7.10. Physical and computer software security must be in place at all times to properly secure access to the recording equipment and video data.

7.11. Video surveillance data may not be publicly viewed or distributed in any fashion as provided by this policy and the *Act*.

7.12. Video data must not be altered in any matter, with the exception of saving investigation material related to an incident required for law enforcement purposes.

7.13. Other than the release to the RCMP, or use for the City of Fernie in accordance with this policy, video surveillance data will only be released on the authority of a warrant to

seize the recorded data for evidence or other court order.

7.14. Any other requests for access to incident specific information must be referred to the FOIPPA Head and will only be disclosed in accordance with the *Act.*

7.15. A Privacy Impact Assessment (PIA) will be conducted and submitted to the Information and Privacy Commissioner (OIPC) where any surveillance program is under consideration.

8. RETENTION AND DESTRUCTION

8.1. Recorded information should be erased every thirty (30) days where no incident of concern to the City has been reported, or where viewing the recorded information reveals no such incident.

8.2. When recorded information (that contains personal information about an individual) reveals an incident and the City uses this information to make a decision that directly affects the individual, the information will be retained for one (1) year after the decision is made.

8.3. Recordings and data which DO NOT contain information pertaining to incident(s) of interest to the City of Fernie as per section 2. General Principles of this policy will be considered to be a transitory record and may be retained for a maximum of thirty (30) days. Once it has been determined that the recording of of no interest, it shall be destroyed immediately.

8.4. Old storage devices must be securely disposed of by shredding, burning or magnetically erasing any and all recorded images and sounds.

8.5. Logs as identified in section 7 Access, Use and Disclosure will have a retention period of the current year plus one year (CY + 1y) and will be destroyed at the expiry of the retention period by authorized personnel, unless otherwise required for legal or other proceedings.

8.6. Reviews and audits as per section 5.1.2 will be retained for a total of eight (8) years (CY + 1y/6y/D).

9. TRAINING

9.1. Where applicable and appropriate, the policy and guidelines will be incorporated into training and orientation programs of the City and service provider(s). Training programs addressing staff obligations under the *Act* will be conducted as considered necessary by the FOIPPA Head.

10. PROCEDURES

10.1. Procedures for Accessing Video Surveillance Records

10.1.1. Video surveillance cameras and recorders are installed for monitoring the downtown core where the safety of public and private assets are of concern, and/or where past crimes have been committed.

10.1.2. The RCMP initiates contact with the Chief Administrative Officer (CAO) or designate in conjunction with an investigation of an alleged crime.

10.1.3. The CAO or designate subsequently views video surveillance recordings for relevant footage.

10.1.4. The CAO or designate provides copies of relevant footage as requested by the authorized RCMP designates.

10.2. Procedures for Maintaining Logs

10.2.1. Detailed logs recording all instances of access to and use of the recording equipment and information collected must be maintained at all times in accordance with this policy.

10.2.2. Locations and times of all recordings must be maintained in logs and kept current with the installation, maintenance and monitoring.

10.3. Procedures for Conducting Audit

10.3.1. Once a video surveillance system has been put in place, an annual audit must be undertaken which assesses if the system is accomplishing its intended purpose.

10.3.2. The annual audit must assess the efficiencies of the equipment, monitoring processes and results. The audit must also evaluate whether the policy is being adhered to and whether unintended negative effects on personal privacy are occurring. Such a review may recommend termination of the system if the intended purposes are not being accomplished or this policy is not being adhered to.

10.3.3. Random audits must also be undertaken to ensure that all authorized personnel is complying with the procedures in accordance with this policy as per section 5.1.2.

10.3.4. If the FOIPPA Head determines that a further review is necessary to be in compliance with the *Act* or this policy, departmental cooperation must be provided.

10.3.5. The FOIPPA Head may also determine that a City employee who is independent of the surveillance system provide a follow-up PIA, including onsite assessments. The FOIPPA Head may recommend termination of the video surveillance system if the intended purposes are not being accomplished, this policy is not being adhered to or if the negative impacts on personal privacy outweigh the benefits of the system.

Legislation Authority:	▪ *Freedom of Information and Protection of Privacy Act, RSBC 1996 Ch. 165*
Related Bylaws, Policies, Procedures, Agreements, etc:	▪ Freedom of Information Bylaw No. 1671, 1994 ▪ Public Places Bylaw No. 2181, 2012 ▪ Use of Cameras and Digital Recording Devices in Public Areas Policy ▪ OIPC Public Surveillance System Privacy Guidelines
Attachments:	▪ Appendix "A" – Privacy Impact Assessment ▪ Appendix "B" – Confidentiality Agreement ▪ Appendix "C" – Access Log

Appendix "A"

PRIVACY IMPACT ASSESSMENT

I BASIC INFORMATION - New or Existing Program, System or Legislation

1. Ministry/Public Body and Program Area.

Ministry	Local Government
Division	City of Fernie
Branch/Section	Corporate Administration Services
Initiative Title	Downtown Surveillance Cameras

2. Contact Position and/or Name, Telephone Number and E-Mail Address.
(This should be the name of the individual most qualified to respond to questions regarding the PIA).

Name, Title	Michelle Martineau, Director of Corporate Administration Services
Branch/Section	
Phone Number	250.423.2231
E-Mail	michelle.martineau@fernie.ca

3. Description of the Program/System/Legislation (Initiative) being assessed.
(Please note here if the initiative does **not** collect, use or disclose personal information). If this is a change to an existing legislation, system or program, describe the current system or program and the proposed changes.

This is a Video Surveillance System that provides continuous or intermittent video recording or video monitoring of selected sites on city sidewalks in the downtown core. The intent of the Video Surveillance System is to deter crime and protect residential and commercial buildings/structures from theft or vandalism.

		*Yes	No
(a)	Does this PIA involve a common or integrated program/activity (as defined in the FOIPP Act)? and		✓
	Is the common or integrated program/activity confirmed by the written requirements set out in the regulation?		✓
(b)	Does this PIA involve a data-linking initiative (as defined in the FOIPP Act)?		✓

If yes, please ensure you have notified the Office of the Information and Privacy Commissioner at an early stage of development of the initiative pursuant to section 69 (5.5) of the FOIPP Act.

4. Purpose/Objectives of the initiative (if statutory, provide citation).

The intent of the City of Fernie's Video Surveillance System in the downtown core is to improve public safety and deter crime such as vandalism, graffiti and other public mischief.

5. What are the potential impacts of this proposal? (Include privacy impacts in this description).

- Public privacy is impacted.
- Images of the public will be captured and retained for a specific period of time before being destroyed.

6. Provide details of any previous PIA or other form of personal information assessment done on this initiative (in whole or in part).

Not applicable – first application.

IF THERE IS NO PERSONAL INFORMATION INVOLVED, GO TO X. SIGNATURES.

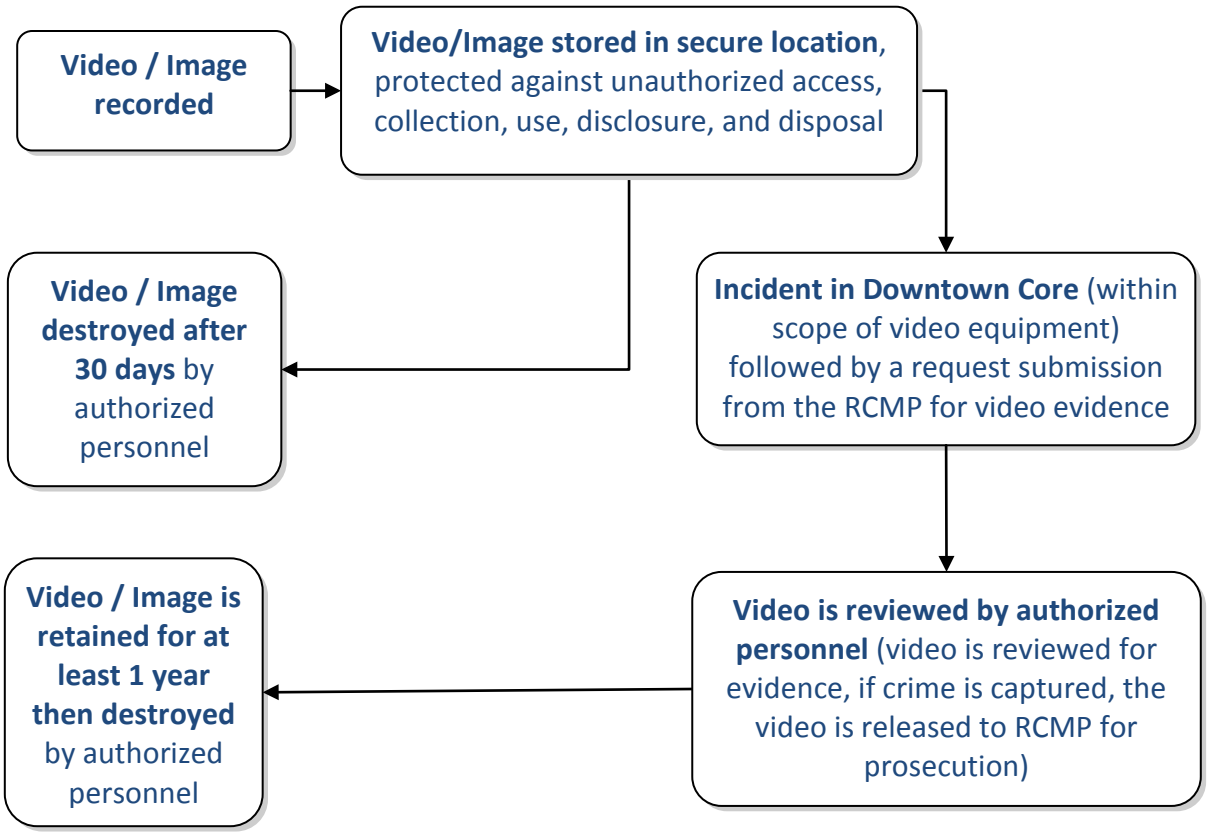
****IMPORTANT NOTE**: The FOIPP Act defines personal information as "recorded information about an identifiable individual other than contact information." Contact information includes the name, title, telephone or facsimile number, email address etc., which enables an individual at a place of business to be contacted.

II DESCRIPTIVE INFORMATION

1. Describe the elements of personal information that will be collected, used and/or disclosed and the nature and sensitivity of the personal information. [See note above about the definition of personal information.]
For example: Name, home address, gender, age/birthdate, SIN, Employee#, race/national, ethnic origin.

- Visual (image of the person – gender, race/national, ethnic origin, body type and shape, features such as hair colour or tattoos)
- Vehicle licence plate number.

2. Provide a description (either a narrative or flow chart) of the linkages and flows of personal information collected, used and/or disclosed.



III PERSONAL INFORMATION COLLECTION

(Section 26 and section 27 of the *Freedom of Information and Protection of Privacy Act* "FOIPP Act")

****IMPORTANT NOTE**: Recent amendments to the FOIPP Act have clarified when personal information has *not* been collected by a public body. See section 27.1 or contact Knowledge and Information Services for further details.

	Yes	No	n/a
Is personal information being collected?	✓		

IF THERE IS NO PERSONAL INFORMATION BEING COLLECTED, GO TO IV. USE OF PERSONAL INFORMATION

1) Authorization for Collection:

A public body may collect personal information as authorized by one of the following provisions:

s. 26		Yes	No	n/a
(a)	Is the collection of personal information specifically authorized by, or under, an Act, other than the FOIPP Act?		✓	
	If yes, please specify the name of the Act and relevant section			
(b)	Is the personal information being collected for law enforcement purposes?	✓		
(c)	Is the personal information directly related to, and necessary for, a program or activity of the public body?		✓	
(d)	Is the personal information being collected for a prescribed purpose (where there is a regulation defining that purpose)?		✓	
	If yes, please specify the prescribed purpose.			
	(i) Has the individual whose personal information is being collected consented, in the prescribed manner, to that collection? **and**			✓
	(ii) Would a reasonable person consider that collection appropriate in the circumstances?			
(e)	Is the collection of personal information necessary for the purposes of planning or evaluating a program or activity of a public body?		✓	
(f)	Is the collection of personal information necessary for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur?		✓	

s. 26		Yes	No	n/a
(g)	Is the personal information being collected by observation at a presentation, ceremony, performance, sports meet, or similar event where the individual voluntarily appears and that is open to the public? **Please identify event:**		✓	
(h)	Is personal identity information being collected by:			
	A designated provincial identity information services provider and the collection of the information is necessary to enable it to provide services under section 69.2, or		✓	
	A public body from a designated provincial identity information services provider and the collection of the information is necessary to enable the public body to identify an individual for the purposes of providing a service to the individual or the provincial identity information services provider to provide services under section 69.2.		✓	

If none of the above questions has been answered "yes", your office does not have the authority under the FOIPP Act to collect the personal information in question. If you have any questions or require clarification please contact Knowledge and Information Services.

2) How will the personal information be collected?

A public body must collect personal information directly from the individual the information is about, with certain specific exceptions.

	Yes	No	n/a
Will the personal information be collected directly from the individual that the information is about?			✓

Information is only being collected through video surveillance equipment; information is not being collected verbally, in writing or through the surrender of legal documents from an individual (just visual images).

IF YOU ARE ONLY COLLECTING PERSONAL INFORMATION DIRECTLY AS NOTED ABOVE, YOU WILL NOT NEED TO COMPLETE THE NEXT SECTION ON INDIRECT COLLECTION. GO TO 3. NOTIFICATION TO COLLECT INFORMATION.

If the personal information has **not been collected directly** from the individual it is about, check which of the following authorizes the indirect collection:

s. 27(1)		Yes	No	n/a
(a)(i)	Did the individual the information is about authorize another method of collection?			✓
(a)(ii)	Has indirect collection been authorized by the Information and Privacy Commissioner?		✓	
(a)(iii)	Has indirect collection been authorized by another enactment?		✓	

s. 27(1)		Yes	No	n/a
	If yes, please specify the name of the Act and relevant section(s)			
(a.1)(i)	Is the personal information necessary for the medical treatment of an individual and it is not possible to collect the information directly from that individual?			✓
(a.1)(ii)	Is the personal information necessary for the medical treatment of an individual and it is not possible to obtain authority under (iv) for another method of collection?			✓
(b)	Is the public body collecting personal information disclosed to it by another public body under an authority within sections 33 to 36 of the FOIPP Act?			✓
	Specify relevant section(s) or subsections that apply.			
(c)(i)	Is the personal information being collected for the purpose of determining suitability for an honour or award including an honorary degree, scholarship, prize or bursary?		✓	
(c)(ii)	Is the personal information being collected for the purpose of a proceeding before a court or a judicial or quasi-judicial tribunal?	✓		
(c)(iii)	Is the personal information being collected for the purpose of collecting a debt or fine or making a payment?		✓	
(c)(iv)	Is the personal information being collected for the purpose of law enforcement?	✓		
(c)(v)	Is the personal information being collected to reduce the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur?		✓	
(d)	Is the personal information being transferred to the public body from another public body in accordance with section 27.1?	✓		
(e)	Is the personal information being collected necessary for delivering a common or integrated program or activity?		✓	
(f)	Is the personal information about an employee, other than a service provider, and the collection of the information is necessary for the purposes of managing or terminating an employment relationship between a public body and the employee?		✓	
(g)	Is the information personal identity information that is collected by the designated provincial identity information service that is necessary to provide services under section 69.2?		✓	
	Additional details as required (e.g., explanation of method of collection) Personal information will be collected through video surveillance equipment installed on selected street light fixtures in the downtown core. Any video records that identify an individual(s) committing a crime may be released to the RCMP upon request as for use in their investigation and may also be used as evidence in a court proceeding.			

If none of the above authorities have been checked, your office does not have the authority under the FOIPP Act to collect the personal information in question **If you have any questions or require clarification** ***please contact Knowledge and Information Services.***

3) Notification to collect information

A public body must ensure that an individual from whom it collects personal information is notified of the collection as outlined below.

27(2)		Yes	No	n/a
	Has the individual from whom personal information is being collected, been informed of:			
	(a) the purpose for collection?	✓		
	(b) the legal authority for collection?	✓		
	(c) the contact information of the person who can answer questions regarding the collection?	✓		
	Additional details as required (e.g., method of notification) Signs shall be posted at the perimeter of the surveillance areas advising the public that the area is under video surveillance and indentify who they can contact to answer questions about the surveillance system.			

Notification is not required if the answer is "yes" to any of the following:

27(3)		Yes	No	n/a
(a)	Is the personal information about law enforcement or anything referred to in section 15(1) or section 15(2) of the FOIPP Act?	✓		
(b)	Has the Minister responsible for the FOIPP Act excused your public body from complying because it would			
	(a) result in the collection of inaccurate information?			✓
	or (b) defeat the purpose or prejudice the use for which the personal information is collected?			✓
(c)	The information (a) is not required, under subsection 27(1), to be collected directly from the individual the information is about, **and** (b) is not collected directly from the individual the information is about			✓
(d)	Is the information collected by observation at a presentation, ceremony, performance, sports meet or similar event at which the individual voluntarily appears and that is open to the public. **Please identify event:**		✓	
27 (4)	Is it reasonable to expect that notifying an employee of collection under subsection 27 (1) (f) would compromise (a) the availability or accuracy of the information, or (b) an investigation or a proceeding related to the employment of the employee?			✓
	Additional details as required Only collected in regards to law enforcement/criminal activity			

If you have not provided the required notification as outlined above, please contact Knowledge and Information Services.

IV USE OF PERSONAL INFORMATION - (Section 32 of the FOIPP Act)

	Yes	No	n/a
Is personal information being used?	✓		

IF THERE IS NO PERSONAL INFORMATION BEING USED, GO TO V. DISCLOSURE OF PERSONAL INFORMATION

Under the FOIPP Act, a public body may use personal information in its custody or under its control only for certain specified purposes as outlined below.

The public body **must** check one or more of the authorities listed below:

s.32		Yes	No	n/a
(a)	Has the individual the personal information is about consented to the use? (Note: Supporting documentation must be on file.)	✓		
(b)	Will the information be used only for the purpose for which it was obtained or compiled or for a use consistent with the original purposes?	✓		
	Please provide details of the original purpose for which the personal information was obtained or compiled. Include, if applicable, details of the consistent/secondary use. Informed consent (signage). Law enforcement and public safety, criminal deterrence. Video records are to be collected only for the purpose of law enforcement and would only be viewed if an incident took place where evidence was needed for prosecution.			
(c)	If the personal information was disclosed to the public body by another public body under an authority within sections 33to 36, is the information being used for that same purpose?	✓		
	Specify subsection(s) being applied 33.1(g) and 33.2(i)			

If you have not checked one of the above, you do not have the authority to use the information.* If you have any questions or require clarification *please contact Knowledge and Information Services.

V DISCLOSURE OF PERSONAL INFORMATION

(Section 33, section 33.1, section 33.2, section 33.3, section 34, section 35 and section 36 of the FOIPP Act)

	Yes	No	n/a
Is personal information being disclosed?	✓		

IF THERE IS NO PERSONAL INFORMATION BEING DISCLOSED, GO TO VI. ACCURACY AND CORRECTION OF PERSONAL INFORMATION.

A public body may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2, or 33.3 of the FOIPP Act.

1) Disclosure of Personal Information

Sections 33, 33.1, 33.2 and 33.3 of the FOIPP Act provide the legislative authority to disclose personal information. Section 33 provides that personal information **cannot** be disclosed unless it is authorized under section 33.1 or 33.2.

Please choose the <u>main</u> authorization(s) for disclosure below. All authorities that <u>may</u> apply do not need to be checked, only the main authorizations for the initiative.

s. 33.1	Disclosure inside OR outside Canada	Yes	No	n/a
(1)(a)	In accordance with Part 2 (pursuant to an FOI request)		✓	
(1)(a.1)	If the information or disclosure is of a type described in section 22(4) (e), (f), (h), (i) or (j): 22(4) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if			
	(e) the information is about the third party's position, functions or remuneration as an officer, employee or member of a public body or as a member of a minister's staff,		✓	
	(f) the disclosure reveals financial and other details of a contract to supply goods or services to a public body,		✓	
	(h) the information is about expenses incurred by the third party while travelling at the expense of a public body,		✓	
	(i) the disclosure reveals details of a licence, permit or other similar discretionary benefit granted to the third party by a public body, not including personal information supplied in support of the application for the benefit, or		✓	
	(j) the disclosure reveals details of a discretionary benefit of a financial nature granted to the third party by a public body, not including personal information that is supplied in support of the application for the benefit or is referred to in subsection 22(3)(c).		✓	
(1)(b)	If the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure inside or outside Canada, as applicable (Note: Supporting documentation must be on file)		✓	
(1)(c)	In accordance with an enactment of British Columbia (other than the *Freedom of Information and Protection of Privacy Act)*or Canada that authorizes or requires its disclosure		✓	
	Specify name of enactment and relevant section(s)			
(1)(c.1)	If the personal information is made available to the public in British Columbia under an enactment, (other than the *Freedom of Information and Protection of Privacy Act*) that authorizes or requires the information to be made public		✓	
	Specify name of enactment and relevant section(s)			

s. 33.1	Disclosure inside OR outside Canada	Yes	No	n/a
(1)(d)	In accordance with a provision of a treaty, arrangement or written agreement that (i) authorizes or requires its disclosure, and (ii) is made under an enactment of British Columbia (other than the *Freedom of Information and Protection of Privacy Act)* or Canada		✓	
	Specify name of enactment and relevant section(s)			
(1)(e)	To an individual who is a minister, an officer of the public body or an employee of the public body other than a service provider, if (i) the information is necessary for the performance of the duties of the minister, officer or employee,		✓	
	and (ii) in relation to disclosure outside Canada, the outside disclosure is necessary because the individual is temporarily travelling outside Canada			
	If paragraph (1)(e)(ii) applies, please explain how the travel is *temporary* and why disclosure outside Canada is *necessary*			
(1)(e.1)	To an individual who is a service provider of the public body, or an employee or associate of such a service provider, if (i) the information is necessary for the performance of the duties of the individual in relation to the public body,			
	and (ii) in relation to disclosure outside Canada, (A) the individual normally receives such disclosure only inside Canada for the purpose of performing those duties, and (B) the outside disclosure is necessary because the individual is temporarily travelling outside Canada		✓	
	If paragraph (1)(e.1)(ii) applies, please explain how the travel is *temporary* and why disclosure outside Canada is *necessary*			
(1)(f)	To an officer or employee of the public body or to a minister, if the information is immediately necessary for the protection of the health or safety of the officer, employee, or minister		✓	
(1)(g)	To the Attorney General or legal counsel for the public body, for the purpose of preparing or obtaining legal advice for the government or public body or for use in civil proceedings involving the government or public body	✓		
(1)(h)	To the minister responsible for the *Coroner's Act* or a person referred to in section 36 of that Act, for the purposes of that Act		✓	
(1)(i)	If			
	(i) the disclosure is for the purposes of collecting amounts owing to the government of British Columbia or a public body by		✓	
	a. an individual, or			

s. 33.1	Disclosure inside OR outside Canada	Yes	No	n/a
	b. corporation of which the individual the information is about is or was a director or officer,			
	and (ii) in relation to disclosure outside Canada, there are reasonable grounds for believing that			
	a. the individual the information is about is in, resides in or has assets in the other jurisdiction, or			
	b. if applicable, the corporation was incorporated in, is doing business in or has assets in the other jurisdiction			
1(i.1)	For the purposes of			
	(i) a payment to be made to or by the government of British Columbia or a public body,		✓	
	(ii) authorizing, administering, processing, verifying or cancelling such a payment, or		✓	
	(iii) resolving an issue regarding such a payment		✓	
(1)(j)	(i) Repealed.			✓
(1)(k)	For the purposes of			
	(i) licensing or registration of motor vehicles or drivers, or		✓	
	(ii) verification of motor vehicle insurance, motor vehicle registration or drivers licences		✓	
(1)(l)	For the purposes of licensing, registration, insurance, investigation or discipline of persons regulated inside or outside Canada by governing bodies of professions and occupations		✓	
(1)(m)	If (i) the head of the public body determines that compelling circumstances exist that affect anyone's health or safety, and (ii) notice of disclosure is mailed to the last known address of the individual the information is about, unless the head of the public body considers that giving this notice could harm someone's health or safety		✓	
(1)(m.1)	For the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur		✓	
(1)(n)	So that the next of kin or a friend of an injured, ill or deceased individual may be contacted		✓	
(1)(o)	In accordance with section 36 (disclosure for archival or historical purposes)		✓	
(1)(p)	The disclosure (i) is necessary for			

s. 33.1	Disclosure inside OR outside Canada	Yes	No	n/a
	(A) installing, implementing, maintaining, repairing, trouble shooting or upgrading an electronic system or equipment that includes an electronic system that is used in Canada by the public body or by a service provider for the purposes of providing services to a public body, or			
	(B) data recovery that is being undertaken following failure of an electronic system that is used in Canada by the public body or by a service provider for the purposes of providing services to a public body		✓	
	and (ii) in the case of disclosure outside Canada (A) is limited to temporary access and storage for the minimum time necessary for that purpose, and (B) in relation to data recovery under subparagraph (i)(B), is limited to access and storage only after the system failure has occurred			
	If paragraph (1)(p)(ii) applies, please explain how the temporary access and storage is for the *minimum time necessary*			
(1)(q)	If the information was collected by observation at a presentation, ceremony, performance, sports meet or similar event at which the individual voluntarily appeared and that was open to the public. **Please identify event:**			✓
(1)(r)	If the information Was disclosed on a social media site by the individual the information is about,			
	Was obtained or compiled by the public body for the purpose of enabling the public body to engage individuals in public discussion or promotion respecting proposed or existing initiatives, policies, proposals, programs or activities of the public body or respecting legislation relating to the public body, **and**			✓
	Is disclosed for a use that is consistent with the purpose described in subparagraph (ii).			
	Additional details as required			
(1)(s)	In accordance with section 35 (disclosure for research or statistical purposes).		✓	
(1)(t)	To comply with a subpoena, a warrant or an order issued or made by a court, person or body in Canada with jurisdiction to compel the production of information		✓	

(2)	In addition to the authority under any other provision of this section or section 33.2, a public body that is a law enforcement agency may disclose personal information referred to in section 33			
(2)(a)	To another law enforcement agency in Canada	✓		

(2)(b)	To a law enforcement agency in a foreign country under an arrangement, a written agreement, a treaty or provincial or Canadian legislative authority.		✓	
(3)	The minister responsible for this Act may, by order, allow disclosure outside Canada under a provision of section 33.2 in specific cases or specified circumstances, subject to any restrictions or conditions that the minister considers advisable.		✓	
(4)	In addition to the authority under any other provision of this section or section 33.2, the Insurance Corporation of British Columbia may disclose personal information if, (a) the information was obtained or compiled by that public body for the purposes of insurance provided by the public body, and (b) disclosure of the information is necessary to investigate, manage or settle a specific insurance claim.		✓	
(5) and (6)	For the purposes of operating the designated provincial identity information services as permitted under section 33.1 (5) and (6)		✓	
(7)	To respond to citizens' enquiries as permitted under section 33.1(7)		✓	
	Additional details as required			

s. 33.2	**Disclosure inside Canada only**	**Yes**	**No**	**n/a**
(a)	For the purpose for which it was obtained or compiled or for a use consistent with that purpose (see section 34)		✓	
	Please provide details of the original purpose for which the personal information was obtained or compiled. Include, if applicable, details of the consistent/secondary use.			
(b)	Repealed.			✓
(c)	To an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of the officer, employee or minister		✓	
(d)	To an officer or employee of (i) a public body, or (ii) an agency or to a minister, if the information is necessary for the delivery of a common or integrated program or activity and for the performance of the duties, respecting the common or integrated program or activity, of the officer, employee or minister to whom the information is disclosed		✓	
(e)	To an officer or employee of a public body or to a minister, if the information is necessary for the protection of the health or safety of the officer, employee or minister		✓	

s. 33.2	Disclosure inside Canada only	Yes	No	n/a
(f)	To the auditor general or any other prescribed person or body for audit purposes		✓	
(g)	To a member of the Legislative Assembly who has been requested by the individual the information is about to assist in resolving a problem		✓	
(h)	To a representative of the bargaining agent, who has been authorized in writing by the employee whom the information is about, to make an inquiry		✓	
(i)	To a public body or a law enforcement agency in Canada to assist in a specific investigation			
	(i) undertaken with a view to a law enforcement proceeding, or	✓		
	(ii) from which a law enforcement proceeding is likely to result	✓		
(j)	To the archives of the government of British Columbia or the archives of a public body, for archival purposes		✓	
(k)	Repealed.			✓
(l)	To an officer or employee of a public body or to a minister, if the information is necessary for the purposes of planning or evaluating a program or activity of a public body		✓	
	Additional details as required			

s. 33.3	Disclosure to Public Without Request	Yes	No	n/a
(1)	Do the records fall within a category established under section 71 (1)?		✓	
	Additional details as required			
(2)	Do the records fall within a category established under section 71.1 (1)?		✓	
	Additional details as required			

2) Systematic or Repetitious Disclosure/Exchanges?

		Yes	No	n/a
i.	Do the disclosures of personal information under section 33.2 occur on a regular basis?		✓	
ii.	Has an Information Sharing Agreement been completed for these disclosures/exchanges?		✓	
iii.	Has information related to the Information Sharing Agreement(s) been entered into the **Personal Information Directory**?			✓

Personal information exchanges within a public body do not normally require an Information Sharing Agreement (ISA) if they are for a consistent purpose as defined under

section 33.2(a) of the Act or are necessary for the performance of an employee of the public body under section 33.2(c). However, depending on the nature and sensitivity of the personal information exchanged, the public body might choose to prepare an ISA or similar written statement of understanding.

3) Research or Statistical Purposes (Section 35)

	Yes	No	n/a
Has a researcher requested access to personal information in an identifiable form for research purposes?		✓	

If "yes", a research agreement that conforms to the criteria established in section 35(d) must be in place. Contact Knowledge and Information Services for assistance.

***Please note*: Research using personal information may only be conducted if it meets all of the terms of section 35.**

4) Archival or Historical Purposes (Section 36)

The archives of the government of British Columbia, the archives of a public body, or a board or a francophone education authority (as defined in the *School Act*) may disclose personal information in its custody or under its control to be disclosed for archival or historical purposes as authorized by section 36.

Please check the authorization(s) for disclosure listed below.

		Yes	No	n/a
(a)	The disclosure would not be an unreasonable invasion of personal privacy under section 22		✓	
(b)	The disclosure is for historical research and is in accordance with section 35 (research agreements)		✓	
(c)	The information is about someone who has been dead for 20 or more years		✓	
(d)	The information is in a record that has been in existence for 100 or more years		✓	

***If you have not answered "yes" to any of the above authorizations for disclosure you do not have the authority to disclose personal information. If you have any questions or require clarification, please contact Knowledge and Information Services*.**

VI ACCURACY AND CORRECTION OF PERSONAL INFORMATION

(Section 28 and section 29 of the FOIPP Act)

If an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body must make every reasonable effort to ensure that the information is accurate and complete. An individual must also have the ability to access, or have corrected or annotated, their personal information for a period of one year after a decision has been made based upon the personal information.

		Yes	No	n/a
1.	Are there procedures in place to enable an individual to request/review a copy of their own personal information?	✓		
2.	Are there procedures in place to correct or annotate an individual's personal information if requested, including what source was used to update the file?			✓
3.	If personal information is corrected, are there procedures in place to notify other holders of this information?			✓
	If yes, please provide the name of the policy and/or procedures, a contact person and phone number.			
	Policy/procedure:	**Video Surveillance Policy**		
	Contact person:	**Michelle Martineau, Director of Corporate Administration Services**		
	Phone number:	**250.423.2231**		
	Additional details as required			

If any of the questions above have been answered "no", please contact Knowledge and Information Services for further clarification.

VII SECURITY AND STORAGE FOR THE PROTECTION OF PERSONAL INFORMATION

(Sections 30 and 30.1 of the FOIPP Act)

Note: For PIAs related to new or existing systems, this section should be completed by the Branch of the ministry responsible for systems maintenance and security, and signed off by this branch, in the Signatures section.

For PIAs that do not involve systems initiatives, this section should be completed by the program area completing the PIA. In this case, the signature of the systems representative is not required.

Section 30 of the Act requires a public body to protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

		Yes	No	n/a
1.	Is there reasonable technical security in place to protect against unauthorized access or disclosure?	✓		
2.	Is there reasonable physical security in place to protect against unauthorized access or disclosure?	✓		
3.	Are there branch policies and procedures in place for the security of personal information during routine collection, use and disclosure of the information?	✓		
	If yes, please provide the name of the policy and/or procedures, a contact person and phone number.			
	Policy/procedure:	**Video Surveillance Policy** **Confidential Information Policy**		

	Contact person:	**Michelle Martineau, Director of Corporate Administration Services**			
	Phone number:	**250.423.2231**			
	Additional details as required				
4.	Have user access profiles been assigned on a need-to-know basis?		✓		
5.	Do controls and procedures exist for the authority to add, change or delete personal information?		✓		
6.	Does your system security include an **ongoing** audit process that can track use of the system (e.g., when and who accessed and updated the system)?		✓		
	Please explain the audit process and indicate how frequently audits are undertaken and under what circumstances Weekly check by Director of Corporate Administration Services s to ensure system is working; ongoing audit to track Video Surveillance System access and destruction of videos after 30 days or after 1 year in the case of prosecutions.				
7.	Does the audit identify inappropriate accesses to the system?		✓		
	Additional details				

If any of the questions above have been answered "no", please contact your Ministry's Security Officer. If you have any questions or require clarification please contact Knowledge and Information Services.

Section 30.1 requires a public body to ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada unless the individual the information is about has consented or the disclosure is otherwise allowable under the Act.

		Yes	No	n/a
	Will the information be stored or accessed only in Canada?	✓		

Personal information in a public body's custody or under its control must be stored and accessed only in Canada, unless one of the following applies:

		Yes	No	n/a
(a)	Has the individual the personal information is about identified it and consented, in the prescribed manner, to it being stored in or accessed from another jurisdiction?			✓
	Please explain			
(b)	Will the personal information be stored in or accessed from another jurisdiction for the purpose of a disclosure that is authorized under the *Freedom of Information and Protection of Privacy Act*?		✓	

	Please explain			
(c)	Will the personal information be disclosed under section 33.1(1)(i.1)?	✓		
	Please explain Section 33.1(g) to legal counsel for use in civil proceedings or legal advice.			

***If you have not answered "yes" to any of the above authorizations for storage or access of personal information outside Canada or if you require clarification, please contact Knowledge and Information Services*.**

VIII RETENTION OF PERSONAL INFORMATION - (Section 31 of the FOIPP Act)

If a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.

		Yes	No	n/a
1.	Do you have an approved records retention and disposition schedule?	✓		
2.	Is there a records retention schedule to ensure information used to make a decision that directly affects an individual is retained for at least one year after use?	✓		

If you answered "no" to the above questions, your procedures may need to be revised. Please contact your Records Officer.

Note: Records of provincial public bodies and designated organizations/public bodies cannot be destroyed unless approval is granted under the authority of the *Document Disposal Act*. Please consult with your Records Officer to initiate the records scheduling process.

Comments:

X SIGNATURES

PUBLIC BODY APPROVAL:

Program Manager	Signature	Date
Ministry Contact Responsible for Systems Maintenance and Security	Signature	Date
Knowledge and Information Services Office of the Chief Information Officer Ministry of Labour, Citizens Services, and Open Government	Signature	Date
Assistant Deputy Minister or Equivalent	Signature	Date

GO TO: PERSONAL INFORMATION DIRECTORY (to add PIA and/or ISA summary)

Appendix "B"

Confidentiality Agreement for Third Parties – Monitoring of Video Surveillance

THIS CONFIDENTIALITY AGREEMENT (the 'Agreement') is dated this __ day of _____, 20__.

BETWEEN: THE CORPORATION OF THE CITY OF FERNIE
501-3rd Avenue, PO Box 190
Fernie BC V0B 1M0

(The "City")

AND NAME OF CONTRACTOR
ADDRESS

(The "Contractor")

NAME OF CONTRACTOR'S DESIGNATED INDIVIDUAL
ADDRESS

(The "Recipient")

OR / AND NAME OF EMPLOYEE
ADDRESS

(The "Employee")

(if applicable) WHEREAS _____ (name of Contractor) has entered into an agreement with the City of Fernie for _____ services at _____. ('the contract site');

(if applicable) AND WHEREAS the Recipient is the individual designated by _____(name of Contractor) who may, from time to time, be asked by the City to monitor recordings made by way of video surveillance at the contract site solely for the purpose of law enforcement as requested by the City;

OR

(if applicable) WHEREAS the Employee may, from time to time, be asked by the City of Fernie to monitor recordings made by way of video surveillance solely for the purpose of law enforcement as requested by the City;

AND WHEREAS the City of Fernie requires that the Recipient/Employee enter into a Confidentiality Agreement prior to accessing personal information contained in the video surveillance recordings;

(if applicable) NOW THEREFORE the Contractor agrees as follows:

1. The Contractor does hereby designate the Recipient as the designated individual for the purposes of this agreement.

2. The Contractor agrees that adherence to this confidentiality agreement and the City's video surveillance policy is the responsibility of both the Contractor and the Recipient and agrees that breach of this confidentiality agreement or non-compliance of the video surveillance policy may result in contract termination.

NOW THEREFORE the Recipient/Employee agrees that:

1. They will keep all information contained in the video recordings strictly confidential and access to such recordings and associated data must be solely for the purposes of law enforcement as requested by the City, and only to the extent required for that purpose;

2. They will keep all video recordings and data secure, not allow access to any other individual or group, and will not make copies of any recordings or data in any format, including electronic formats, unless given written and explicit approval by the City's Head of Freedom of Information and Protection of Privacy;

3. All information shared with the Recipient/Employee is governed by the *Freedom of Information and Protection of Privacy Act* (The "*Act*") and that the Recipient/Employee will abide by the terms of this Act;

4. All recordings and data provided to the Recipient/Employee must be returned to the City promptly after use, must be viewed and returned within one week of receipt, and must not be destroyed by the Recipient/Employee. The Recipient/Employee must not keep any copies of such recordings and data in any format, including electronic formats;

5. They will ensure the security and integrity of the recordings and data, and will keep them in a physically secure and separate location safe from loss, alteration, destruction, intermingling with other records and data, and access by any unauthorized individuals;

6. At all times, they will take all reasonable precaution to prevent inadvertent use, copying or transferring of the data or information provided by the video recordings and will not email or otherwise transmit the recordings or data in any format;

7. They will not disclose, divulge or communicate in any way to any person, firm or corporation, including but not limited to the Contractor or any other employees of the Contractor, any information of which the Recipient/Employee becomes aware of by means of accessing such recordings and data and will observe strict secrecy in regards to that information;

8. They will promptly deliver all data and recordings, in all media formats provided, to the City upon completion of any task performed by request of the City.

9. All recordings and data and any information from such recordings and data shall at all times remain the exclusive property of the City;

10. They will abide by the City's Video Surveillance Policy as attached to this Agreement and as updated from time to time. The Recipient/Employee agrees that breach of this confidentiality agreement or non-compliance of the video surveillance policy may result in termination of employment or termination of contract.

11. They will immediately inform the City if they receive notice that they may, or will, be legally required to disclose video recordings or data in their possession, or to disclose information regarding recordings or data. Prior to disclosing any information, the City must be consulted so that, if necessary, they can attempt to prevent or limit such disclosure.

12. The Recipient/Employee's obligations under this Agreement are to remain in effect perpetually and will exist and continue in full force and effect regardless of whether the Recipient is no longer a designated individual for the Contractor or the Contractor is no longer providing the services to the City OR the Employee is no longer an employee of the City.

IN WITNESS WHEREOF the parties have signed this agreement as of the day and year above first written.

CITY OF FERNIE

_____

(Print name)
Head, Freedom of Information and
Protection of Privacy

CONTRACTOR/EMPLOYEE

_____

(Print name)

RECIPIENT

_____

(Print name)

Appendix "C"

Access Log Sheet for Video Surveillance System

Camera Location	**Date of Recording**	**Time of Recording**	**Date of Viewing**	**Reason for Viewing Recording**	**Name of Viewer** (Please Print)	Signature of Viewer

Note: To be retained by the City of Fernie till the end of the current plus 1 year after the last entry, unless otherwise required for legal or other proceedings.