POLICY

Policy No. 26 – 303 – 16/10/17
Department: Bylaw Enforcement

PUBLIC VIDEO SURVEILLANCE

SCOPE:

- The Town of Nanton recognizes the need to balance an individual's right to privacy against the Town's duty to promote a safe environment for all citizens, and to protect town property and employees, by means of surveillance camera the use of which is both lawful and justifiable.
- This policy applies to video surveillance activities necessary to enhance the security and safety of people and property on Town-owned premises. This policy will only apply to Town owned property that is being leased or rented to a tenant with the consent of the leasee or tenant.
- This policy has been created in accordance with the Alberta Freedom of Information and Protection of Privacy Act Guide to Using Surveillance Cameras in Public Areas, which outlines the obligations of local public bodies with respect to the protection of the privacy of individuals.

PURPOSE:

- Develop a surveillance system policy to regulate the use of video surveillance and recording on Town owned property that complies with the Freedom of Information and Protection of Privacy Act.
- Information obtained through video surveillance will be used exclusively for security and law enforcement purposes, which must relate to the protection of the public or the deterrence or detection of criminal activity, including theft, vandalism, or other property damage.
- Ensure consistency of Town of Nanton surveillance measures.
- These guidelines do not apply to covert or overt surveillance cameras being used as a case-specific investigation tool for law enforcement purposes or in contemplation of litigation. They are also not intended to apply to workplace surveillance systems installed to conduct surveillance of employees.

1. DEFINITIONS:

1.1 **Covert Surveillance** refers to the secretive continuous or periodic observation of person, vehicles, places or objects to obtain information concerning the activities of individuals.

1.2 **FOIP** means the *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, and any amendments thereto.

1.3 **Overt Surveillance** refers to the non-secretive continuous or periodic observation of person, vehicles, places or objects to obtain information concerning the activities of individuals.

1.4 **Personal Information** is defined in section 1(1)(n) of FOIP as recorded information about an identifiable individual. It includes the individual's race, colour, national or ethnic origin; the

individual's age or sex; the individual's inheritable characteristics; information about an individual's physical or mental disability; and any other identifiable characteristics listed in that section.

1.5 **Reception Equipment** refers to the equipment or device used to receive or record the personal information collected through a surveillance system, including a video monitor.

1.6 **Record** is defined in section 1(1)(q) of FOIP as a record of information in any form and includes books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records.

1.7 **Storage Device** refers to a videotape, computer disk or drive, CD ROM or computer chip used to store the recorded visual images captured by a surveillance system.

1.8 **Surveillance System** refers to a mechanical or electronic system or device that enables continuous or periodic video recording, observing or monitoring of personal information about individuals in open, public spaces, public buildings or public transportation.

1.9 **Town** as referred to in this Policy, shall include all departments and employees, as well as any agency of Town Council which has agreed to be bound by this Policy.

2. POLICY:

2.1 Installation of Surveillance Equipment

a) Reception equipment such as video cameras may be installed in identified public areas where surveillance is a necessary and viable detection or deterrence activity.

b) Reception equipment shall not be positioned, internally or externally, to monitor areas outside a building, or to monitor other buildings, unless necessary to protect external assets or to ensure personal safety. Cameras should not be directed to look through the windows of adjacent buildings.

c) Equipment shall not monitor any areas where the public and employees have a reasonable expectation of privacy.

d) Consideration should be given to the use of surveillance being restricted to periods when there is a demonstrably higher likelihood of crime being committed and detected in the area under surveillance. Only those persons responsible, as per this policy, should have access to the system's controls and to its reception equipment.

e) Reception equipment should be in a controlled access area. Only the employee responsible, as per this policy, should have access to the reception equipment. Video monitors should not be located in a position that enables public viewing.

f) The video surveillance system and the process for maintenance of the system will be subject to periodic assessment by the Chief Administrative Officer.

2.2 Public Awareness Of Cameras

a) Reception equipment locations and operation shall be limited to visual access of areas where there is no reasonable expectation of privacy. Video surveillance for the purpose of monitoring work areas, social areas, or sensitive areas will only occur in special circumstances, and must be consistent with the policy's principle purpose, which will include the prevention / deterrence of illegal activity and the enhancement of safety.

b) Appropriate signs and notice of video surveillance must be posted in areas subject to video monitoring.

c) Unless the public has otherwise been made aware of surveillance cameras at a surveillance area, the main entrance of the area will display a notice as follows, or with similar content:

Surveillance cameras may be operating in <location of camera> to deter and/or detect criminal activity and for public security. The collection of recorded camera images is authorized under section 33(c) of the Freedom of Information and Protection of Privacy Act (FOIP) Act. If you have any questions about this surveillance, contact <name of position> at <phone number>.

d) In addition, the following notice, or one with similar content, will be displayed at the surveillance location:

Surveillance camera may be operating in this area to detect and/or deter unlawful activity (vandalism, theft) and for public security. For more information, contact <name of position> at <phone number>.

2.3 Limiting Use and Disclosure Of Personal Information

a) Employees will have access to information collected through video surveillance only where necessary in the performance of their duties and in accordance with the provisions of this policy.

b) Employees who may require access to information collected through video surveillance will be provided proper training and orientation with regards to this Policy and their obligations under this Policy and FOIP, and will provide written acknowledgement that they have read and understood the contents of this policy and procedure. Any employee who knowingly or deliberately breaches this policy or FOIP will be subject to discipline up to and including termination.

c) All storage devices that are not in use should be stored securely in a locked receptacle located in a controlled access area. All storage devices that have been used should be numbered and dated.

d) Access to the storage devices should only be by employees responsible as per this policy.

e) A logbook will be kept with regard to the use of each recording device. Storage Devices will only be removed when an incident occurs. The employee responsible for this task will take control of the storage device in question and secure it in a sealed envelope with the time and date of the seizure and initials of the employee on the seal of the envelope.

f) An individual who is the subject of the information has a right to access to his or her recorded information. Access may be granted in full or in part depending upon whether any of the exceptions in FOIP apply and whether the excepted information can reasonably be severed from the record.

2.4 Retention of Information

a) The guidelines for retention of recorded information is supplementary to the Town of Nanton's Records Retention Bylaw.

b) All recording medium must be handled in a manner that maintains the integrity and security of the recorded information.

c) All recorded information shall be retained for a minimum of three months.

d) All recorded information used in conjunction with the provisions of this policy, shall be retained for a minimum of one year after using it so that the individual identified has a reasonable opportunity to obtain access to it, or for a shorter period of time as agreed to in writing by the individual.

e) Information specifically awaiting review for detection of possible criminal activity or non-compliance with or breach of a statute or bylaw that could lead to a penalty or sanction, shall be retained and stored for a minimum of one year.

f) If the recorded information, which has detected possible criminal activity or non-compliance with a breach of a statute or bylaw is requested by a law enforcement agency, the recorded information will be submitted to the law enforcement agency and will become a record in custody of that agency. The agency must complete a release form, provided by the Town in respect to this policy, prior to removal of the information from the Town's custody. The release form shall be filed by the Town's Administration for retention as per current practices.

g) Old storage devices must be securely disposed of by shredding, magnetically erasing, or otherwise permanently deleting the information, and must be recorded as such as per the current record retention bylaw.

3. RESPONSIBILITIES:

3.1 Council to:

a) approve this Policy and any subsequent amendments.

3.2 Department Heads to:

a) ensure the requirements of this Policy are adhered to;
b) establish and maintain an internal reporting network relating to control mechanisms and advise the CAO;
c) budget for the costs of their video surveillance requirements;

3.3 Chief Administrative Officer to:

a) conduct periodic assessments to ensure compliance with this policy.
b) assist Department Heads with the administration of this Policy;
c) ensure that any new legislation pertaining to the use of video surveillance is incorporated into this Policy, as required;
d) review all proposed changes to existing video surveillance systems and newly proposed systems to ensure that they meet all the requirements of this Policy; and determine who shall have access to view storage devices.

3.4 Employees to:

a) review and comply with this Policy in performing their duties and functions related to the operation of a surveillance system;

b) attend training relating to this Policy, where available.

MAYOR

October 17, 2016
Date

CHIEF ADMINISTRATIVE OFFICER

October 17, 2016
Date