COMMUNITY SAFETY DEPARTMENT
GUIDELINES FOR THE USE OF VIDEO SURVEILLANCE

PREAMBLE:

The Community Safety Department has a duty to promote and maintain a safe and secure environment for students, staff and visitors at York University. The Department uses video surveillance, also known as closed-circuit television (CCTV) surveillance, to:

- Enhance the safety of individuals and the security of assets and property;
- Prevent, deter, reduce the fear of, and detect criminal activity;
- Summon emergency assistance or deploy security resources;
- Help first responders (i.e. police, fire and paramedic vehicles) navigate across campus;
- Verify alarms and door access control systems; and
- Assist law enforcement in investigations and prosecutions of criminal activity, including identifying suspects and potential witnesses.

These guidelines have been developed by the Department to ensure that it collects, uses, discloses, retains and disposes of personal information in compliance with the *Freedom of Information and Protection of Privacy Act* (FIPPA) and to ensure that the Department balances the protection of individuals and assets with the protection of privacy. These guidelines complement and build on those outlined by York University's Information and Privacy Office and the Information and Privacy Commissioner of Ontario's *Guidelines for the Use of Video Surveillance* (2015).

WHO SHOULD USE THESE GUIDELINES?

These guidelines are to be used by all Department staff, including employees and contractors, who are involved in the installation, monitoring and management of video surveillance devices and records that are within the custody or under the control of the Department.

These guidelines do **not** apply to video cameras used for:

- ***Permitted educational, research and teaching purposes;***
- ***Lawful creative expression;***
- ***Non-security purposes*** (e.g. recording athletic events for public relations aims); or
- ***Personal use by a private person or third-party entity*** that is not acting under the authority of the University and is operating a video camera that is not within the custody or control of the University (e.g. subway stations and businesses on campus, such as stores in York Lanes). Privately-owned-and-operated cameras are the sole responsibility of the user. Anyone who violates a reasonable expectation of privacy risks liability under criminal law or civil law and sanctions.

SECTION 1: DEFINING NECESSITY

Under FIPPA, York University can collect personal information when necessary to the proper administration of a lawfully authorized activity. York University has authorized the Department to manage the operation of its video surveillance system.

Under these guidelines, “necessity” is defined as more than merely helpful. In evaluating whether video surveillance is necessary, the Department will examine the totality of contextual factors, including:

- ***The safety problem***. Use of video surveillance is justified based on verifiable safety concerns.
- ***Alternatives***. Less intrusive ways to achieve the same goals are substantially less effective than video surveillance or are not feasible.
- ***Proportionality***. The benefits of video surveillance substantially outweigh the reduction of privacy inherent in its use.
- ***Sensitivity of information***. Sensitivity is based on the nature of the space under observation and the closeness of the video surveillance. The greater the sensitivity of information collected, the greater the benefit must be to justify video surveillance.
- ***Amount of information***. The amount of personal information collected is limited to the minimum amount necessary to meet the safety and security objective. For example, to minimize privacy intrusion, video surveillance cameras will **not** collect audio information.
- ***Additional relevant factors***. Each situation is assessed uniquely considering factors such as, cultural sensitivities, values, diversity, differential impact on marginalized or vulnerable communities and consultation feedback from stakeholders, where feasible.

The Department has an unwavering commitment to support free and open exchange of ideas and opinions by all members of the community through respectful debate. The purpose of using video surveillance is **not** to intimidate or interfere with, obstruct, prevent, restrain or disrupt the exercise of any lawful right or freedom, such as the right to peacefully protest or the right to freedom of expression.

The Department must be able to demonstrate that it made an informed decision and will evaluate the necessity of video surveillance on an ongoing basis.

SECTION 2: INSTALLATION OF VIDEO SURVEILLANCE CAMERAS

All requests from the York community for installation, relocation or removal of video surveillance cameras should be submitted to the Department for approval. Assessment of the quantity, type and specific placement of the cameras will vary due to several variables, including:

- ***Area of concern***. What is to be viewed or recorded;
- ***Level of security risk***. More video surveillance cameras may be needed in areas of higher risk; and
- ***Serviceability***. Ease of future access for maintenance.

Video surveillance cameras will **not** be positioned to look through windows or adjacent property, or those areas will be blocked from view or blacked out. If video surveillance cameras are adjustable, these capabilities will be restricted, to the extent possible, so that operators cannot monitor unintended areas.

Video surveillance cameras will **not** be installed to monitor areas where a person has a reasonable expectation of privacy, such as washrooms, change rooms or private residence living spaces. Video surveillance cameras will be installed to monitor public areas, such as building exteriors, points of entry or exit, library interiors (e.g. circulation areas, study rooms and computer labs), hallways, walkways, alleys, streets, loading docks, parking areas and athletic fields or audience seating.

The Department will **not** install dummy (e.g. fake/non-functioning) video cameras.

SECTION 3: VIDEO SURVEILLANCE MONITORING

Because community members may be present at all hours of the day, the Department's video recording systems may operate at any time in a 24-hour period. All video surveillance monitors will be in a secure, access-controlled area.

Prior to being granted authority to monitor video surveillance, Department staff will:

1. Provide the Department with a Criminal Record Check and a Vulnerable Sector Check, with a satisfactory result; and
2. Sign a written confidentiality agreement.

The Department will use and disclose video surveillance for safety and security purposes:

- The Department will **not** use video surveillance to monitor employee or student performance; and
- An individual's or a group's behaviour may warrant monitoring with safety in mind. However, the Department will **not** selectively monitor people in a discriminatory way based on an Ontario *Human Rights Code* protected ground (e.g. age, ancestry, citizenship, colour, creed, disability, ethnic origin, family status, gender identity, gender expression, sex, sexual orientation, marital status, place of origin or race).

The video surveillance system does not provide complete coverage of all areas on campus. Also, although some video surveillance will be live monitored, most video surveillance records will only be viewed when a security incident is reported or suspected. *For these reasons, Community members **cannot** rely on the video surveillance system to provide absolute safety.*

SECTION 4: NOTICE OF COLLECTION

Notice of collection of personal information will be provided on the Department's website. The following information will be easily accessible:

1. The legal authority for the collection of personal information;
2. The principle purpose(s) for which the personal information is intended to be used; and
3. The title, business address and business telephone number of a public official who can answer questions about the collection of personal information.

The Department will prominently display signs at the perimeter of monitored areas and at key locations within the areas to provide notice that video surveillance is, or may be, in operation.

SECTION 5: DISCLOSURE AND ACCESS TO RECORDS

The Department will only disclose records if lawfully permitted to do so, such as:

- In compelling circumstances affecting the health or safety of an individual;
- To a law enforcement agency in Canada to aid an investigation undertaken with a view to a proceeding or from which a proceeding is likely to result;
- To employees who need access to perform their duties and where access is necessary and proper in the discharge of the University's functions; and
- When required by law.

When a law enforcement agency requests access, they must submit a Release of Information form to the Department and provide:

- The case occurrence number;
- The name, contact information and badge number of the investigating officer; and
- A description of the requested information.

If access is authorized, then the following will be logged on the Release of Information form:

- The date of release;
- The name of the Director of Security Services or designate who authorized disclosure;
- The name of the Department staff member who released the record; and
- The name and badge number of the officer that disclosure was made to.

Copies of records for purposes of a criminal investigation will be dated and labelled with a unique, sequential number or other verifiable symbol. To maintain a proper audit trail, logs will be kept of all instances of access to these copies.

Other access requests that are not from law enforcement are subject to the approval of the York University Information and Privacy Office.

SECTION 6: RETENTION AND DISPOSAL OF RECORDS

The Department will take reasonable measures to ensure the secure storage and disposal (e.g. by overwriting, shredding, burning or magnetic erasing) of records in its custody or under its control. Storage devices (e.g. CD, DVD or hard drives) that are not in active use will be locked in a controlled-access area:

- Records that have not been accessed or disclosed will automatically be overwritten when the hard drive is full (typically ranging from two weeks to two months); and
- Records that have been accessed or disclosed will be kept for at least one year.

Department staff will not attempt to alter, conceal or destroy a record, or cause any other person to do so, with the intention of denying a right of access.

SECTION 7: PRIVACY BREACHES

Privacy is breached when personal information is collected, used, disclosed or retained in a manner that is inconsistent with FIPPA.

Department staff will <u>immediately</u> report a suspected or confirmed privacy breach and non-compliance of these guidelines to their immediate supervisor (or, if unavailable, the next level of management) and the Director of Security Services.

The Director of Security Services (or designate) will notify the York University Information and Privacy Coordinator who will address the potential breach. For additional information, see:

- Reporting Privacy Breaches: Guidelines for York University Units
  http://ipo.info.yorku.ca/files/2015/01/Privacy-Breach-Guidelines.pdf

- Privacy Breach Report Form
  http://ipo.info.yorku.ca/files/2015/02/Privacy-Breach-Report-Form.pdf

CONTINUOUS IMPROVEMENT:

These guidelines have been established to provide direction for the Department's use of video surveillance. The Department will periodically undertake a risk-based, self-assessment audit to ensure adherence to these guidelines, and will also review and update these guidelines as needed. Any suggestions for improvements to the guidelines should be sent by email to: safety@yorku.ca.