NORTHERN LIGHTS COLLEGE

Video Surveillance

Policy Number:	A-5.17
Category:	Administration
Effective Date:	February 10, 2017
Approval Process:	Administrative
Approval Date:	February 9, 2018
Date Last Reviewed:	February 10, 2017

POLICY

Video and audio surveillance systems are inherently privacy invasive. As such, Northern Lights College (College) recognizes the need to strike a balance between the individual's right to be free from the invasion of privacy and the institution's duty to promote a safe environment for all community members.

This policy shall not apply to 'law enforcement' activities by Federal, Provincial or Municipal law enforcement agencies.

PURPOSE

The College recognizes that it may obtain personal information only if the information relates directly to and is 'necessary' for a program or activity of the public body.

As such, the purpose of this policy is to ensure that the installation and use of surveillance equipment at the College be authorized by the College and shall comply with the Freedom of Information & Protection of Privacy Act (FIPPA) and other applicable legislation within Canada.

Specifically, surveillance shall be used to monitor the safety of students, employees and individuals accessing College property, and of property and assets.

SCOPE

The effectiveness of a surveillance system is not a one size fits all solution. The use of surveillance at the College has been designed to collect the minimum amount of 'personal information' necessary.

The scope of surveillance may be inclusive across all College locations. This includes campus surveillance systems at Dawson Creek, Fort St. John, Chetwynd, Tumbler Ridge, Fort Nelson, Dease Lake, and Atlin.

PROCEDURE

(1) Use:

(a) The College will consider surveillance as a visual deterrence. However; the College recognizes that this deterrent may be short-lived. As such, the deployment of the

surveillance systems will coincide with the installation of improved lighting and increased monitoring and intervention.

(b) The College shall identify and record verifiable, specific incidents of crime, public safety concerns or other compelling circumstances and will use surveillance as an investigative tool, only if there is no other viable alternative.

(c) Surveillance shall not be used in areas of privacy (i.e. washrooms, first aid rooms, or residence private living quarters), but may be considered for use in public workspaces in accordance with the above.

(d) Video surveillance will not be used to routinely monitor employee productivity or performance; however, recordings may be accessed and viewed on an exceptional basis if and when required to investigate incidents raising concerns about personal safety, damage to property, a contravention of college policy, or a contravention of the law.

(2) Installation & Operation:

(a) The Director of Facilities shall:

(i) approve and oversee the installation and/or decommissioning of video cameras and reception equipment;

(ii) approve the location of the reception equipment, which shall be in a controlled access area(s) and shall not be located in a position that enables public access or viewing;

(iii) establish a schedule of operations of the surveillance equipment; and

(iv) ensure that decommissioned surveillance equipment and recordings will be disposed of according to FIPPA requirements.

(b) The Director of Facilities will ensure that all areas under video surveillance will be publicly identified by way of a sign and/or the symbol of the security service provider. Also, a surveillance "as-built" map for each campus will be available upon request.

(c) For internal purposes, a campus map illustrating the location of the video surveillance cameras will be kept with the Director of Facilities and updated as required.

(3) Records Storage/Retention/Disclosure:

(a) Unused storage devices (including tapes, computer disks, and memory storage devices) shall be stored securely in a locked receptacle.

(b) Recorded information will be erased according to a standard retention and disposal schedule. Retention periods will be no longer than 30 days, although circumstances may necessitate different retention periods.

(c) If recorded information reveals an incident that contains personal information about an individual, and the College uses this information to make a decision that directly affects the individual, s. 31 of FIPPA requires that specific recorded information be retained for one year after the decision is made.

(d) Access to recorded surveillance and/or storage devices must be approved by the Director of Facilities and/or the FIPPA Officer. Access may be granted to Campus Administration (or delegates of Campus Administration) for material recorded on Northern Lights College property.

(e) Authorities requiring access to or release of records/storage devices for risk management, legal and/or evidentiary purposes shall complete and submit a written request to the Director of Facilities and/or the FIPPA Officer before any storage device or recordings shall be disclosed or released in accordance with the FIPPA. The request shall include the name of the requestor, the reason for the request, to whom it was released, under what authority, and if it will be returned or destroyed after use.

(f) With FIPPA, an individual who is the subject of surveillance, has the right to request access to his/her recorded personal information. Request for access shall be in writing to the Director of Facilities and/or the FIPPA Officer and shall be processed in accordance with the FIPPA.

(g) The College shall securely dispose of old storage devices. The storage media shall be burned, shredded, or magnetically erased.

(4) "New" Requests for Surveillance Installations:

(a) A College representative shall meet with and provide copies of a written request for surveillance to the Director of Facilities and/or the FIPPA Officer detailing the reason for the request and attaching backup documentation.

(b) The Director of Facilities shall complete detailed and comprehensive assessment(s), prior to approving and installing surveillance.

(c) If approved, copies of the assessment(s), the case for implementing surveillance as per above and an approved surveillance plan shall be filed with the Director of Facilities and/or the FIPPA Officer.

(5) Ongoing Evaluation:

(a) The effectiveness of a video surveillance system will be regularly evaluated. Some considerations for evaluation include:

(i) taking special note of the initial reasons for undertaking surveillance and determine whether video surveillance has in fact addressed the problems identified;

(iii) reviewing whether a video or audio surveillance system should be terminated, either because the problem that justified its use in the first place is no longer significant, or because surveillance has proven ineffective in addressing the problem; and

(iv) taking account of the views of different groups in the College affected by the surveillance.

DEFINITIONS

Personal Information: FIPPA defines 'personal information' as recorded information about an identifiable individual, other than contact information. Video and audio recordings of an individual's image and voice are considered identifiable information.

Collection: In terms of surveillance systems, "collection" of personal information occurs when an individual's image or voice is captured by the system. The personal information may then be played back or displayed on a monitor (used), saved or stored (retained) or shared with other public bodies or organizations (disclosed). Surveillance systems are collecting person information whenever they are recording, regardless of if, or how, the public body uses, retains or discloses the recordings in the future.

Law Enforcement: Section 26(b) of FIPPA authorizes collection of personal information for the purposes of law enforcement. Schedule 1 of FIPPA defines 'law enforcement' as: policing, including criminal intelligence systems; investigations that lead or could lead to a penalty or sanction being imposed; or proceedings that lead, or could lead, to a penalty or sanction being imposed.

"Policing" is not defined in FIPPA, however in common law the definition of policing involves active monitoring or patrolling in order to deter or intervene in unlawful activities. Information collected for policing purposes must be collected be a public body with a common law or statutory enforcement mandate. For example, it is not sufficient for a public body to claim an interest in reducing crime in

order to justify collection for "law enforcement"; the public body must have authority to enforce those laws.

In British Columbia, the Office of the Information and Privacy Commissioner has determined in a number of Orders that an investigation must already by underway at the time the personal information is collected for Section 26(b) to apply. A public body is not authorized to collect personal information about citizens, in the absence of an investigation, on the chance it may be useful in a future investigation. Similarly, in order for a collection to be lawfully authorized as relating to a proceeding, the proceeding must be ongoing at the time of collection.

Necessary: Section 26(c) of FIPPA authorizes the collection of personal information that is necessary for an operating program or activity of the public body. 'Necessary' in the context of surveillance systems is a high threshold for a public body to meet. It is not enough to say that personal information would be nice to have or could be useful in the future. The personal information must also be directly related to a program or activity of the public body.

STAKEHOLDERS

Board of Governors and Northern Lights College Executive
Northern Lights College Faculty and Staff
Northern Lights College Students

RELATED POLICIES

- A-5.18: Sexual Violence and Misconduct

REFERENCES

- Office of the Information and Privacy Commissioner – Public Sector Surveillance Guidelines, January 2014
- Freedom of Information and Protection of Privacy Act
- Human Rights Act
- Northern Lights College and BCGEU Collective Agreement

History

Created/Revised/Reviewed	Date	Author	Approved By
Created	February 10, 2017	Todd Bondaroff	Policy Committee
Revised	February 9, 2018	Todd Bondaroff	Policy Committee

Next Scheduled Review Date

February 2019 (Annually)