

Video Surveillance Policy

Category: Operations

Approval: PVP

Responsibility: Director, Risk Management

Date: November 5, 2013, Last Revised February 23, 2018

Definitions:

Reception equipment: any device capable of capturing and/or recording images, including audio and thermal imaging devices.

Video Surveillance System: refers to a video, physical or other mechanical, electronic, digital or wireless surveillance system or device that enables continuous or periodic video recording, observing or monitoring of specific locations on Trent University property and the actions of individuals in those locations.

Personal Information: is recorded information about an identifiable individual which includes, but is not limited to, the individual's race, colour, national or ethnic origin, sex and age.

Purpose/Reason for Policy:

This purpose of this policy is to regulate the use of video surveillance and recording on Trent University property.

Information obtained through video surveillance will be used primarily for safety, security and enforcement purposes, which relate to the protection of students, staff, faculty, and the public, the deterrence or detection of illegal activity, including theft, vandalism, or other property damage or the contraventions of university policies.

Scope of this Policy:

Video surveillance may be used for purposes relating to safety of individuals and security of buildings and property. In furtherance of these purposes, video surveillance may be used to monitor exterior and interior areas of Trent property where there is no reasonable expectation of privacy.

This policy only applies to video surveillance activities necessary to enhance the security and safety of people and property on Trent premises. This policy does not apply to Trent owned property that is being leased or rented to a tenant.

This policy has been created in accordance with the Guidelines for Using Video Surveillance

Cameras in Public Places as issued by the Information and Privacy Commissioner of Ontario, September, 2007 and the Ontario Freedom of Information and Protection of Privacy Act (the Act), both of which outline the obligations imposed on institutions with respect to the protection of the privacy interests of individuals.

Policy Statement:

Video surveillance of Trent premises will be conducted in a professional, ethical and legal manner, in accordance with the following principles:

- (a) Video surveillance must be conducted in accordance with the laws of Ontario and Canada;
- (b) Video surveillance will be used only where it is demonstrably necessary for the purposes of enhancing the safety of persons, the deterrence of theft or destructive acts, such as vandalism and graffiti, or the enforcement of university policies, such as parking regulations. Video surveillance may also be used administratively to conduct car counts in parking lots.
- (c) Video surveillance will be used only by Campus Security or Trent employees authorized by the Director, Risk Management, and only where less intrusive means of deterrence, such as monitoring by Security Guards, has been shown to be ineffective or unworkable.
- (d) Appropriate signs and notice of video surveillance must be posted in areas subject to video monitoring;
- (e) Employees and video service provider(s) 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.
- (f) Employees and video service providers 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 the Act, and will provide written acknowledgment that they have read and understood the contents of this policy and procedure. Any employee who knowingly or deliberately breaches this policy or the Act will be subject to discipline up to and including termination. Failure of a video service provider to comply with this policy or the Act will constitute breach of contract and may result in termination of contract and legal action.
- (g) The recording medium must be handled in a manner that maintains the integrity and security of the recorded information;
- (h) All recorded information shall be destroyed within three months excepting information specifically awaiting review by law enforcement agencies, information seized as evidence, or information that has been duplicated for use by law enforcement agencies.
- (i) 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 include the prevention/deterrence of
 illegal activity and the enhancement of safety;
- (j) When video surveillance footage is being displayed by authorized employees on a video monitor, the monitors should be in a position that cannot be viewed by others.
- (k) The video surveillance system will be subject to periodic audit.

Responsibilities:

Security Guards, Dispatchers, Parking and Risk Management Staff are responsible to operate and monitor the video surveillance system(s) when and as directed.

The Security Manager is responsible to manage and coordinate maintenance of the video surveillance system(s), train employees who will access the system and ensure that the system is used in accordance with this policy.

The Director, Risk Management is responsible for oversight of the system, especially with respect to privacy issues, arranging periodic audits of the system and recommending new video installations and system upgrades through the budget process.

Contact Officer:

Director, Risk Management

Date for Next Review:

February 2023

Related Policies, Procedures & Guidelines

- a) Video Surveillance Procedures
- b) Policy on the Protection of Personal Information

Policies Superseded by This Policy:

a) Not Applicable