SAINT MARY'S UNIVERSITY SINCE 1802

One University. One World. Yours.

Name:	Video Recording and Surveillance Policy
Policy Number:	3-1058
Origin:	Facilities Management
Approved:	November 19, 2015
Issuing Authority:	Senior Director Facilities Management
Responsibility:	Manager University Security
Revision Date(s):	n/a
Effective Date:	November 19, 2015

1. Introduction:

Saint Mary's University (the "University") recognizes the need to strike a balance between the individual's right to privacy and the University's duty to promote and maintain a safe and secure environment for students, staff, faculty and visitors.

The use of closed circuit television surveillance systems (CCTV) results in the collection of personal information in the form of images and records of the conduct of individuals.

CCTV systems are employed by the University to record unlawful conduct and breaches of relevant University policies, such as the Code of Conduct as well to prevent and deter such conduct.

Images of activities performed by employees in the workplace and that are captured/recorded by CCTV cameras will NOT be used for any disciplinary or other labour relations purpose as specified within the confines of any/all collective agreements in force between Saint Mary's University and its employees/employee groups.

2. Purpose:

The purpose of this policy is to regulate the use of Surveillance Equipment, including closed circuit television cameras and other monitoring and recording equipment systems used to monitor and record public and restricted areas of Saint Mary's University property, for the purposes of enhancing the security and safety of students, faculty, staff and the protection of physical property of the University.

3. Definitions:

"Surveillance Equipment" means any closed circuit television cameras and any other video/image monitoring and recording equipment systems used to monitor and record public and restricted areas on Saint Mary's University property. This also includes any system to monitor and record an individual's identifying information when accessing public and restricted areas on Saint Mary's University property.

"Senior Director" means the Senior Director of Facilities Management.

"Manager" means the Manger of University Security.

"CCTV" means a Closed Circuit Television System.

"Camera" is a devise that converts images into electrical signals for television transmission, video recording, or digital image.

4. Responsibilities:

Saint Mary's University Security Services is responsible for Saint Mary's University's CCTV program, including ensuring proprietary CCTV systems comply with the terms and conditions of the policy.

University Security will:

a) Monitor all CCTV cameras and maintain a suitable monitoring station in a controlled, high-security area with access restricted to Security Services.

b) Ensure that all recordings are kept in a locked receptacle located in a controlled access area. Each storage device that has been used will be dated and labeled with a unique, sequential number or other verifiable symbol.

c) Ensure that the implementation and operation of all CCTV Systems comply with this policy.

d) Ensure that appropriate signage is in place at all entrances to the University advising of the use of CCTV cameras and providing contact information for the person responsible for the program.

e) Ensure all personnel monitoring the CCTV cameras are appropriately trained and supervised in the responsible use of cameras and recording equipment.

f) Manage the secure storage and tracking of all images including copied data recordings required for investigative/or evidence purposes.

g) Be responsible for the disclosure of all images.

The following persons shall be authorized to access live images and recordings of past images, but only from cameras in their area:

a) Senior staff managing the Gorsebrook Pub

b) Senior staff managing the Residences

c) Senior staff managing the Food Service Operations

d) Student Residence Service Officers authorized by the Senior Director, Student Services or the Director, Housing & Conference Services, and under the supervision of the Director, Housing & Conference Services and Assistant Director, Residence Services.

5. Policy:

a) Subject to this Policy, Saint Mary's University Security has the sole authority to oversee and coordinate the use of all surveillance Equipment on Saint Mary's University Campus.

b) Video/images monitoring and recording under this Policy will be designed and operated in a manner that minimizes privacy intrusion and that is absolutely necessary to achieve lawful goals.

c) Information obtained through video/image monitoring or recording will be used for University security, safety and law enforcement purposes only.

d) All information obtained through video/image monitoring and recording is confidential and will only be released when authorized by the Manager of University Security.

e) All persons involved in the use of Surveillance Equipment at Saint Mary's University will be appropriately trained and supervised in the responsible use of this technology.

6. Procedures:

6.1. Installation of Surveillance Equipment:

The authorization for the installation of Surveillance Equipment lies with the Manager of University Security. No one is authorized to install, or arrange to be installed, any Surveillance Equipment unless such installation has been approved in advance by the Manager.

a) Departments wishing to install CCTV systems or to monitor CCTV systems shall make a request to the Manager of University Security. All CCTV device installations must be approved by the Manager of University Security

b) All CCTV installation requests shall be reviewed by the Security Manager who will determine best practices, advice on locations.

c) The University will make every effort to position cameras so that they only cover University premises or occupied spaces.

d) CCTV cameras will be installed in public areas, such as hallways, common areas, parking lots and walkways.

e) Video surveillance for the purpose of monitoring work areas or sensitive areas should only occur in special circumstances where approved by the Manager of University Security.

f) Where CCTV is to be installed in Residence areas the Director of Housing and Conference Services will be involved.

g) All CCTV areas will be marked with signage to ensure that people entering the area are aware that video recordings are in operation, except in circumstance related to approved covert cameras.

6.2. Exclusions

This policy does not apply to:

a) Use of video recording and CCTV technology covered by University policies governing research with human subjects or animals.

b) Use of CCTV technology by the Fred Smithers Centre of Support for Students with Disabilities to monitor center exams. There will be no recording of any images.

7. Public Awareness of Surveillance Equipment:

a) In locations where Surveillance Equipment is in use, signs must be posted in an appropriate area, either at the entrance to the area under surveillance or in close proximity to the camera.

b) If the Surveillance Equipment is recording, the following sign will be displayed:

> This area is being RECORDED by closed circuit television.

8. Covert Surveillance:

a) Covert surveillance (hidden camera without signage) will be used only be used in exceptional cases and with the approval of the Senior Director.

b) Where it appears that covert surveillance may be required, the Manager will first conduct an assessment of the specific circumstances of the situation and make a recommendation to the Senior Director.

c) The Manager's assessment must clearly demonstrate that covert surveillance is the only available option in the circumstance that the benefits derived from the information obtained would far outweigh the violation of privacy of the individuals observed and that covert surveillance is not otherwise a violation of the law.

d) Surveillance Equipment will be positioned in a way that minimizes unnecessary surveillance (e.g. in the case of an ongoing computer theft problem, the camera will be positioned so that the individuals will be recorded only if they approach the equipment of concern).

e) In all cases, covert surveillance will be time limited.

9. Requests to view recordings:

a) Only trained individuals working for Saint Mary's University Security are permitted to operate Surveillance Equipment and access live or recorded material. However, in exceptional circumstances, the Manager may designate other specific individuals at Saint Mary's University to operate Surveillance Equipment and access live or recorded material.

b) All requests by University administrators or law enforcement agencies to view recorded information must be made to and are subject to the approval of the Manager. Where permission is granted to view recorded material, that material must be viewed in the presence of a trained individual working at Saint Mary's University Security. The request to view must pertain to an investigation commenced by Saint Mary's University Security or an outside law enforcement agency.

c) All other requests to view recorded information must be made as a Freedom of Information and Protection of Privacy application to the appropriate authority.

10. Safeguards:

a) All recordings produced by Surveillance Equipment will be kept in a secure manner or locked facility and managed appropriately by Information Technology Systems and Support (ITSS) to protect legal obligations and evidentiary value.

b) If a copy of a recording must be made for evidentiary purposes. It must be copied onto permanent storage medium (such as a CD or DVD) and physically labeled with a date, time and location of the surveillance. No other copies of

surveillance recordings, other than those needed for back-ups or evidentiary purposes may be made.

c) Recordings from surveillance cameras will be kept for a maximum of 30 to 90 days unless otherwise required for the purposes outlined in the policy. Recordings will be erased or otherwise destroyed at that point unless retained as part of a criminal investigation or court proceedings (criminal or civil), or other bona fide use as approved by the Manager.

11. Disclosure of Images:

a) Information obtained through video monitoring shall be used exclusively for security and law enforcement purposes.

b) No attempt shall be made to alter any part of a recording

c) Video recordings will not be shown or provided to anyone other than Security Services or approved personnel except in the following circumstances:

   i. Law enforcement agencies for the purpose of an investigation.

   ii. For use at a formal University proceeding such as a Student Code of Conduct hearing.

   iii. To assist in the identification of individuals relating to a criminal incident.

   iv. To comply with a Freedom of Information request by the person whose identity has been recorded who shall have the right to access such information.

   v. Other circumstances as approved by the Manager of University Security.

d) Disclosure of video recordings to third parties will only be made in accordance with the purpose(s) for which the system was installed, and will be limited to:

   i. Police and other law enforcement agencies, where the images could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder.

   ii. Prosecution agencies.

   iii. Relevant legal representatives.

   iv. People whose images have been recorded and retained, unless an exemption applies.

   v. In exceptional cases, to assist in the identification of a victim, witness or perpetrator in relation to a criminal incident.

   vi. Members of staff involved in University disciplinary processes.

12. Accountability:

A log will be kept by University Security with regard to use of Surveillance Equipment. The log will reflect all instances where:

a) A member of University Security or person designated by the University Security Manager views a recording

b) A request is made to view a recording.

c) The Manager denies a request to view a recording and the reason why.

d) The Manager permits an individual to view a recording (this will include the reason the request was granted, who viewed the recording, when, and who from University Security was present during the viewing), and

e) The Manager releases a recording to a law enforcement agency.

13. Annual Report

The Manager will provide an annual report to the Senior Director of Facilities Management, regarding this policy. The report will include:

a) All requests to install new Surveillance Equipment.

b) All new Surveillance Equipment installations.

c) The removal of Surveillance Equipment.

d) Recommendations for revisions to the Policy, if necessary.

e) Any other information which may be relevant to the operation of this Policy.

14. Non-Compliance with this Policy

Any non-compliance of this policy by departments, individuals or third party suppliers shall be reported to the Manager of University security

The Manager will review all reports of non-compliance and advise the Senior Director of facilities Management to determine the appropriate resolution or sanctions.