



APPROVED

Administration Council

14 July 2016

GUIDELINES ON CAMERA SURVEILLANCE SYSTEMS

Rationale

The safety and security of the campus and the members of the Lasallian community are of primary importance. Technological advances in safety and security include the use of closed-circuit television (CCTV) or camera surveillance systems.

The objectives of De La Salle University in using camera surveillance systems are:

- a. To aid in safety and security operations in campus;
- b. To capture information that could be used to investigate crimes, such as theft and vandalism;
- c. To use surveillance as a means of deterring crimes;
- d. To aid in providing information to the members of the community for such cases as traffic, flood, and crowd build-up; and
- e. To comply with regulatory requirements.

However, to curb the predisposition to look at CCTVs as the be-all, end-all solution to security concerns and to minimize the potential misuse and abuse of these privacy-invasive devices, there is a need to promulgate these guidelines to communicate policies and procedures relating to CCTVs.

Principles

1. The privacy of individuals in the campus shall be of primordial consideration.
2. Personal information should not be collected unless the information is collected for a lawful purpose connected with a function or activity of the school and the collection of the information is necessary for that purpose.
3. Personal information collected should be protected against loss, access, use, modification, or disclosure and other misuse
4. Personal information collected may be only be used and disclosed for the purpose that it was collected (except in certain specific circumstances)

Policies

5. Upon written recommendation by any office head indicating the proposed location and position of the camera surveillance system, the Director of the Security Office shall make an initial assessment based on the factors below:
 - 5.1 Necessity. Less intrusive means of deterrence have shown to be ineffective or unworkable in the area to be covered.
 - 5.2 Risk level of area. The area to be covered is considered high risk in terms of security, safety, theft and vandalism because of its physical circumstances.



- 5.3 Positioning of camera. CCTVs should not be directed to look through the windows of adjacent properties and should not cover the interior of areas where students, staff and the public have a well-understood expectation of privacy.
- 5.4 Consultation with affected parties
- 5.5 Mandated specifications, as established in statutes or regulations
6. The Vice Chancellor for Administration shall make the final decision on the installation of the CCTV based on the assessment of the Director of the Security Office.
7. The following must be observed in installing CCTVs:
 - 7.1 Monitors or reception equipment should not be located in areas that allow public viewing and should be strictly in a controlled access area.
 - 7.2 Camera surveillance systems should not be used to monitor staff performance.
 - 7.3 The standard signage (in yellow, with the words "Notice: CCTV in operation") must be affixed in the general area covered by the CSS.
8. The storage of and access to CCTV footage shall adhere to the following:
 - 8.1 A command center, staffed with individuals competent/trained in CCTV operations, shall be maintained on a 24/7 basis.
 - 8.2 Live feed from camera surveillance systems may be made accessible through the internet, on a need basis, subject to the approval of the Vice Chancellor for Administration.
 - 8.3 The mandatory retention period for recorded data from camera surveillance systems is fifteen (15) calendar days.
 - 8.4 Access to handle storage devices should be limited to authorized personnel. A list of those with access to storage devices should be prepared and approved by the Vice Chancellor for Administration.
 - 8.5 Access to recorded data may be requested by any member of the Lasallian community, by any law enforcement agent with mission order, by court order, or by any interested party either as part of hot pursuit or for the purpose of evidence, when the incident is more than one hour passed.
 - 8.5.1 In cases of hot pursuit, the Director, Security Office may grant access for the viewing of CCTV footage to the requesting party. No copy of the footage may be made or released.
 - 8.5.2 In cases when the purpose is to gather evidence, as requested through a formal request, the Vice Chancellor for Administration shall make the final decision, upon the recommendation of the Director, Security Office.



- 8.6 Purging or removal of recorded information must be done on a regular basis by authorized personnel and must be documented.

Approved in the Administration Council meeting on 14 July 2016, for implementation effective 31 July 2016.