UNIVERSITY OF DUBLIN
TRINITY COLLEGE

CODE OF PRACTICE

CODE OF PRACTICE REGARDING THE OPERATION OF CLOSED CIRCUIT TELEVISION CAMERAS FOR SECURITY OR OTHER PURPOSES IN TRINITY COLLEGE DUBLIN

Approved by Board: 16 September 2009

1. Background

1.1. It is now approximately ten years since the decision was taken to install CCTV cameras on Campus on the advice of the Gardai in order to provide enhanced protection for students, staff and visitors as well as College buildings and facilities in the context of an open campus. The Finance Committee, the Site and Facilities Committee and the Board approved this decision at the time. A Code of Conduct was drafted and a monitoring committee comprised of representatives of students and staff was appointed to assuage any concerns which members of the College Community may have had at the time in relation to this decision.

1.2. While the technology used in to-day's CCTV systems has changed considerably from that available ten years ago the principles in terms of the purposes for which CCTV systems are used, the operation and control of the systems and College's concern for the protection of the rights and privacy of the individual remain unchanged.

2. CCTV Systems

The College CCTV coverage is now comprised of three different types of systems as follows:

2.1. Main Campus System. The External Campus CCTV System. This system is comprised in the main of external CCTV cameras located around the Campus which are monitored and recorded on a 24 hour basis in the Security Centre at 201 Pearse Street. There are a small number of internal cameras also linked into this system. The College Facilities Officer and the Chief Steward have day to day operational responsibility for this system.

2.2. Internal CCTV Systems. The second type of CCTV system [in use in buildings on and off Campus] is a system consisting of a number of cameras located within a building which are monitored and recorded locally within the building at the attendant reception desk. Monitoring is only possible during hours when there is an attendant present but recording is on a 24 hour basis. The College Facilities Officer and the Campus Superintendent have day to day operational responsibility for these systems.

2.3. 'Webcam' Systems. The third type of CCTV system in use in College is a 'Webcam' based system. This system is comprised of a number of web cameras linked to a computer hard disk which records footage on a pre-determined basis depending on local circumstances and requirements. These systems are departmental, school or building based systems and day to day operational control and responsibility lies with the 'Head' of the department, school or building in question.

3. Principles Governing the Operation of CCTV Systems

3.1. All CCTV systems under College control must operate in compliance

with:

- Current legislation covering Data Protection and Freedom of Information

- This Code of Practice.

3.2 The main purpose of CCTV systems in the College is to assist in the maintenance of security [principally the protection of life and property], to facilitate proceedings in the context of criminal or legal issues, including the investigation of major staff or student disciplinary offences – see paragraph 6.6. below. CCTV cameras may also be used for purposes other than security, eg., as part of a research project, for the purpose of recording the progress of a large building project or for monitoring the performance of important items of equipment or machinery.

3.3. In the operation of CCTV camera systems, the College will have the greatest possible regard for the protection of the fundamental right to privacy enjoyed by each staff and student member of the College as well as visiting members of the public, and their rights of free association and free expression within the law. CCTV cameras will not be used with the intention of monitoring or recording student union or trade union activities in College. Those charged with the operation of the various CCTV systems in College must exercise the greatest possible care and ensure that the systems are not used in any unauthorised or inappropriate manner.

3.4. Notices will be placed in prominent locations throughout the Campus and in buildings indicating that CCTV cameras are in use.

3.5. A Monitoring Committee comprised of two Group of Unions representatives, representatives of the two Student Unions, the Staff Relations Manager and the Facilities Officer will be appointed to monitor compliance with this Code of Practice. This committee will replace the previous Monitoring Committee established under the Code of Practice adopted in 1996.

4. Data Controller.

4.1. The Data Protection Acts require that a Data Controller be appointed to manage and control data generated as a result of the operation of CCTV systems. The College Data Controller is the Secretary to the College. All CCTV systems in College, irrespective of the purpose for which they are installed, fall within the remit of the Data Controller and must be operated in

compliance with this Code of Practice. The installation of all CCTV systems in College must have the prior approval of the Data Controller. This principle applies irrespective of the intended purpose of the system or the type of cameras or recording arrangements proposed. Therefore, schools, departments, offices or other units in College intending to install a local CCTV system within their building(s) or area of operation must seek prior approval from the Data Controller.

4.2. The College Facilities Officer is responsible for ensuring that the main Campus CCTV system and internal CCTV systems [in buildings serviced by attendant staff] are operated in compliance with this Code of Practice.

4.3. Where an internal CCTV system is in operation in a building without attendant staff the Person in Control of the building [where one has been appointed] or the Head of the principal school, department or unit is responsible for ensuring that the system is operated in compliance with this Code of Practice.

4.4. Where a Webcam CCTV system is in operation in a building the Person in Control of the building [where one has been appointed] or the Head of the principal school, department or unit is responsible for ensuring that the system is operated in compliance with this Code of Practice.

5. Recording

The signals received from the cameras on the main Campus system and the internal building systems are recorded on digital video recorders [DVRs], and the recordings are retained on the DVRs for a period of time, usually between fourteen and twenty eight days after which they are automatically erased. The length of time that recordings are stored varies depending on the capacity of the DVR hard disk and the number of cameras connected to the particular system. In the case of the webcam system the same arrangements apply except the recordings are retained on a computer hard disk. The principle is adopted that if recordings do not produce relevant images then they should be deleted, or recorded over, within 28 days – [attention is drawn to the Paragraph 6 below detailing the conditions governing access to recordings].

6. Access to CCTV Recordings.

6.1. Governing Principles. Irrespective of which of the three systems is in place, or the purpose for which the system was installed, the same governing principles [detailed above] apply in terms of the restrictions on the use and purposes for which the CCTV system may be employed and the same controls govern access to recorded footage. All recorded footage will be properly secured, ie., access controlled by password managed by the Person

in Charge of the System.

6.2. Security Cameras. In the case of CCTV cameras installed for security and safety purposes access to recordings will only be granted in situations where such access is legitimately required, in relation to the investigation of possible criminal activities, the investigation of serious health and safety issues, eg., fires or fire hazards, the investigation of major staff or student disciplinary offences [see paragraph 6.6 below] or to provide evidence for legal proceedings. Recorded footage which does not contain relevant images should be erased from DVRs or hard disks or recorded over within 28 days.

6.3. Access to recordings. Access to recordings will only be given on foot of a request for authorisation from the Chief Steward to the Data Controller – see Annex 'A'. Where authorisation is granted it will be given in writing and a copy of the authorisation will be retained on file by the Chief Steward.

6.4. Research. In the case of CCTV cameras installed for research purposes access to recorded footage will be controlled by the Research Project Manager for the particular project and will in any case be restricted initially to those persons directly and necessarily involved in the project. Recordings may only be used for research purposes and may not be subsequently used for other purposes. Any recorded footage which may thereafter form part of research findings being made accessible for general academic purposes must take account of the privacy rights of persons captured in the recordings. Recorded footage not required as part of the research project should be erased from DVRs or hard disks or recorded over within 28 days.

6.5. Building Projects. In the case of CCTV cameras installed for the purposes of monitoring building projects, equipment or machinery access to recorded footage will be controlled by the Building Project Manager for the particular project, equipment or machinery and will in any case be restricted to those persons directly and necessarily associated with the project, equipment or machinery. Recordings may only be used for the stated purpose and may not be subsequently used for other purposes. Any recorded footage which may subsequently be made accessible to others for legitimate work related purposes must respect the privacy rights of any persons captured in the recordings. Recorded footage not required for the stated purpose should be erased from DVRs or hard disks or recorded over within 28 days.

6.6. Investigations. Recordings will not be used in relation to the investigation of staff or student disciplinary matters, other than matters which may involve criminal or legal proceedings, or major student or staff disciplinary offences as referred to in the University Statutes, Chapter XII, Schedules II and 111.

7. Downloading Recorded CCTV Footage.

7.1. The following procedure will apply where access to recorded footage is authorised by the College Data Controller (Secretary) in connection with security matters or to facilitate proceedings in the context of criminal or legal issues.

7.2. The relevant footage will be downloaded onto a DVD or tape by the Chief Steward or Deputy Chief Steward.

7.3. A copy of the downloaded footage will be retained in a secure location by the Chief Steward and the second copy will be handed over to the Gardai or other authorized agency as provided for under this Code of Practice. The Chief Steward will retain the footage in question until the case is concluded at which point the footage will be erased.

8. Breach of Procedure.

Where it is alleged that a breach of the procedures contained in this Code of Practice has occurred the matter should be reported by the complainant to the College Data Controller (Secretary). Thereafter, in consultation with Staff Office, an investigation will be established to ascertain the facts following the existing procedures agreed with the various staff and student representative bodies. Depending on the outcome of the investigation it may be necessary to establish a formal disciplinary hearing. Any such disciplinary hearing will be conducted in accordance with the relevant College disciplinary procedure.

Annex 'a'

Chief Steward's Office,

Regent House,

Trinity College

Date:

Secretary to the

College.

Permission to view CCTV Footage.

Dear Secretary,

Permission is requested to allow
……
to view CCTV footage held on
the……system in connection

with……
……

Yours Sincerely

_____

Chief Steward.

Permission Granted / Not Granted.

_____

Secretary to the College (Data Controller).