Data Protection Guidelines

Closed Circuit Television Surveillance Systems at DCU

DATA PROTECTION GUIDELINES
FOR CLOSED CIRCUIT TELEVISION SURVEILLANCE SYSTEM AT DCU

1 GENERAL

The CCTV System ("the System") comprises a number of cameras installed at strategic locations around the campus at DCU, both inside and outside buildings.

The purpose of this Guideline document is to support the objectives of the System, and to outline how it is intended to fulfil these objectives.

The system is managed by the Estates Office Security Services Section.

1.1 Purpose and Objectives of CCTV at DCU

Surveillance of public places and the buildings to:-

- Assist in the prevention and detection of crime or disorder
- Reduce the fear of crime or disorder
- Facilitate the apprehension and prosecution of offenders in relation to crime and disorder
- Enhance employee, student, contractor and visitor safety
- Assist with Traffic Management
- Preserve life and property

1.2 General Principles

The System will be operated in line with requirements set out in the Data Protection Acts 1988 and 2003 as well as DCU Data Protection Policy & Procedure.

The System will be operated fairly and only in line with the purposes for which it was established or as subsequently agreed in accordance with these Guidelines.

The System will be operated with due regard to the privacy of individuals.

It is intended, as far as reasonably possible, that these Guidelines will balance the objectives of the System with the need to safeguard the individual's right to privacy.

1.3 Function and Position of Cameras

All of the cameras produce monochrome or full colour pictures, and are fixed or have a pan tilt and zoom (PTZ) capability. The camera movement also has the ability to be permanently restricted to prevent intrusion into private property where appropriate.

The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the System.

Cameras will not be used to look into private residential property. Privacy zones may be programmed into the system as required in order to ensure that the interior of any private residential property within range of a camera is not surveyed.

1.4 Function of Monitoring Equipment

The equipment has the capability of recording all camera pictures simultaneously throughout every 24-hour period. At DCU images from every camera may be recorded throughout the 24-hour period of every day (subject to correct functionality).

The Monitoring Equipment enables the Estates Office to record the images from selected cameras, produce hard copies of recorded images, replay images or copy pre-recorded images from hard drive to portable media as required and in accordance with these Guidelines.

1.5 Signs

Signs are placed at main entrance points to the campus. The signs indicate:-

- The presence of CCTV
- Contact Telephone number of the Estates Office
- The purpose for which CCTV is in operation

1.6 Complaints

Any member of the public wishing to register a complaint with regard to any aspect of the System may do so by contacting the Estates Office. Any such complaint will be dealt with in accordance with DCU procedures. In the event of a complainant not being satisfied with the outcome of their complaint investigation, the complaint may be referred to the Data Protection Commissioner.

1.7 Changes to the Guidelines

Changes to this document may only be made by the Estates Office and must be in accordance with DCU's overall Data Protection Policy.

1.8 Copyright

Copyright and ownership of all material recorded by virtue of the System will remain with DCU.

2 OPERATION OF CCTV MONITORING EQUIPMENT

2.1 General

The CCTV Monitoring Equipment at DCU will be operated in accordance with the terms set out in this document. The operators will be specifically selected for the role and will be trained in the use of the equipment. Each operator will be personally issued with a copy of these Guidelines. They will be fully conversant with the contents of this document, which may be updated from time to time, and which he/she will be expected to comply with at all times.

Monitoring shall be conducted by a trained operator. An authorised operator will be present at all times when the monitoring equipment is in use.

2.2 Responsibilities

The Estates Office accepts primary responsibility for ensuring there is no breach of security and that these Guidelines are complied with and has day-to-day responsibility for the management of the monitoring equipment.

Any breach of these Guidelines or any aspect of confidentiality or security will be dealt with in accordance with established DCU disciplinary procedure.

2.3 Access to CCTV Monitoring Equipment

For reasons of security and confidentiality, access to the CCTV Monitoring equipment is restricted. Only those members of staff, trained specifically as CCTV operators will be allowed to operate any of the equipment.

Unauthorised access by staff is prohibited and Operators should enforce this requirement at all times and with due care.

Public access to the designated location of the CCTV monitoring equipment will be prohibited except for lawful, proper and sufficient reasons and only with the authority of a Security Services Supervisor. Any such visits will be conducted and recorded in accordance with these Guidelines. Any person wishing to see the designated CCTV monitoring equipment locations may apply to do so through the Estates Office.

Visits by auditors may take place at any time, without prior warning. However, auditors must be able to identify themselves as such to a Security Services Supervisor. Any such visit should immediately be notified to the Security Services Superintendent.

2.4 Operation of CCTV Cameras

The operators of the cameras will act with utmost probity at all times.

Every use of the cameras will accord with the purposes and key objectives of the System and shall be in compliance with these Guidelines. It shall be the responsibility of system operators to ensure that the system is operated in accordance with the policy.

Cameras will not be used to look into private property. 'Privacy Zones' may be programmed into the system as required in order to ensure that the interior of any private property within range of the System is not capable of being surveyed by the cameras.

Camera operators will be mindful of exercising prejudices, which may lead to complaints of the System being used for purposes other than those for which it is intended. The operators may be required to justify their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the audit of the System or by the Security Services Superintendent.

Primary Control: Only those members of staff with responsibility for using the equipment will have access to the operating controls, those operators having primacy of control at all times.

Secondary Control: Under no circumstances will the recording of information gathered from the System take place anywhere other than the designated CCTV monitoring equipment location at DCU.

3 HANDLING OF RECORDED MATERIAL

3.1 General

All recorded material (including downloads to portable media and prints) will be handled with care and in a confidential manner.

For the purposes of these Guidelines, 'recorded material' means any material recorded by, or as a result of, technical equipment which forms part of the System, but specifically includes images recorded on hard drive and by way of copying to portable media including video prints.

Every hard disk image, recorded CD etc. used in conjunction with the System has the potential of containing recorded material which may be admitted in evidence at some point during its lifespan.

Members of the community should have total confidence that information recorded about their ordinary, everyday activities by virtue of the System will be treated with due regard to their individual privacy.

It is therefore of the utmost importance that each hard drive/CD etc. is treated strictly in accordance with these Guidelines. Every movement and usage must be meticulously recorded.

Access to, and the use of, recorded material will be strictly for the purposes defined in these Guidelines only.

Recorded material will not be copied, sold or used for commercial purposes or the provision of entertainment.

3.2 Access to Recorded Material

Every request for the release of personal data generated by this System will be channelled through the Security Services Superintendent.

The showing of recorded material to members of the public will take place only in accordance with the law and with authorisation of the Security Services Superintendent.

Recorded material will only be disclosed to (a) an individual on receipt of a written Subject Access Request and once it has been identified as being the person shown on the images; (b) to the Gardaí upon request and proper identification or (c) to Estates Office Management.

Members of the Gardaí (or other law enforcement agencies) have a statutory authority to investigate and/or prosecute offences and recorded material may have to be disclosed to them on a specific written request. They may also release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses. Any Gardaí request should be referred to the Security Services Superintendent.

Recorded material should under no circumstances leave the campus unless when being handed over to law enforcement agencies on written request or to a data subject on a written subject access request.

3.3 Retention

Recorded material will be retained for up to 28 days.

Each set of copied recorded material written to portable media will have a unique tracking sheet, which will be retained for at least three years after the data has been destroyed. The tracking sheet will be retained by the Security Services Superintendent.

3.4 Evidential Information

Any requests for a copy of the recorded material being required for evidential purposes are to be immediately referred to the Security Services Superintendent.

3.5 Video Prints

A video print is a copy of an image or images, which already exist on the hard drive. Video prints will not be taken as a matter of routine. Each time a print is made it must be capable of justification by the originator who will be responsible for recording the full circumstances under which the print is taken (e.g. as part of an individual Subject Access Request/legitimate Gardaí request, internal investigation of suspected criminal activity etc.)

Video prints contain data and will therefore only be released once approval is given by the Security Services Superintendent. All prints that are produced will be recorded and notified to the Security Services Superintendent who will maintain a record of such prints.

4 MONITORING AND AUDIT

The Estates Office has day-to-day responsibility for the monitoring operation.

The Security Services Superintendent will be responsible for regularly auditing the operation of the System and the compliance with these Guidelines. Audits, (which may be in the form of irregular spot checks) will include examination of the monitoring equipment and the content of recorded images.

5 APPENDIX I – CERTIFICATE OF AGREEMENT

The content of these Guidelines is hereby approved in respect of the System, and, as far as reasonably practicable, will be complied with by all who are involved in the management and operation of the System.

SIGNED: _____

Michael Kelly
Director of Estates

DCU Data Protection Guidelines for CCTV		
Estates Office Security Services Section		
Approved by:	Date	
V1.0 - Michael Kelly (Director of Estates)	03/04/2014	