ULSTER UNIVERSITY
CCTV POLICY

1. Closed Circuit Television (CCTV)

These guidelines (the "**Policy**") set out the terms governing the use and management of the CCTV equipment and images in order to ensure the University's compliance with the Data Protection Act 1998 (the "**DPA**"), Human Rights Act 1998 and other relevant legislation.

This Policy is in line with the Information Commissioner's CCTV Code of Practice, a copy of which is available online at:
http://ico.org.uk/for_the_public/topic_specific_guides/cctv

1.1 Purpose

The University has installed the CCTV system for the following purposes (the "**Purposes**"):

1.1.1 to deter crime;

1.1.2. to assist in the prevention and detection of crime;

1.1.3. to assist with the identification, apprehension and prosecution of offenders;

1.1.4 to assist with the identification of actions that might result in disciplinary proceedings being taken against staff or students and in giving evidence to relevant members of staff where disciplinary action may be or is being taken; and

1.1.5 to identify car parking and traffic management problems at the campuses.

1.2 Covert Recording

1.2.1. In certain limited and exceptional cases, the University may be required to carry out covert recording (i.e. use the CCTV scheme to monitor individuals without alerting them to the fact).

1.2.2 Covert recording may only be undertaken with the written authorisation of the Director of Physical Resources, or in his absence his nominated deputy.

1.2.3. Any such monitoring will only be carried out for a limited and reasonable amount of time consistent with the objectives of the monitoring, and only for a specific unauthorised activity.

1.2.4. The monitoring must be necessary in order to obtain evidence of that specific unauthorised activity.

1.2.5. The use of signage must be likely to prejudice the purposes for the covert recording (i.e. the success of obtaining evidence of an unauthorised activity).

1.2.6. The covert recording should only take place over a specific time period and should not continue after that time period has expired or the investigation has ended. Any monitoring which is likely to be oppressive must be limited unless there are overriding reasons for doing so.

1.2.7. Covert recording should not be used in areas where individuals expect privacy (such as bathrooms) unless there is a real suspicion of serious crime and an intention to involve the police.

1.2.8. Any information that is not relevant to the main purpose of the covert recording should be disregarded and, where possible, deleted.

1.2.9. All such activities will be fully documented showing the reason/s leading to the decision to use covert recording and who made the decision.

1.3 Cameras

1.3.1 The University will make every effort to position cameras in order that they only cover University premises and will be in a position to record images relevant to the Purposes.

1.3.2. If for any reason, any neighbouring domestic areas that border the University's property are included in the camera view, the relevant people will be consulted prior to any recording, or recording for those areas will be disabled/masked.

1.3.3. The University will clearly and visibly display signs so that staff, students and visitors are aware that they are entering an area covered by CCTV.

1.3.4. Signs will state:

1.3.4.1 the University is responsible for the CCTV scheme;
1.3.4.2 the Purposes; and
1.3.4.3. who to contact regarding the CCTV scheme.

1.4. Quality of Images

1.4.1. Images produced by the CCTV equipment must be as clear as possible in order that they are effective for the Purposes.

1.4.2. The University will ensure that the cameras are checked, maintained and cleaned on a regular basis to ensure the integrity of the images. The University shall retain a record of all maintenance work carried out to the CCTV system.

1.5 Processing of Images - Retention and Security

1.5.1 Integrity of Images

Recording media must register the correct time and date.

1.5.2. Analogue Recording Systems

CCTV images recorded on a hard drive will be kept for a period of 31 days.

1.5.3. Digital Recordings

1.5.3.1. Digitally recorded CCTV images held on the hard drive of a PC or a server will be overwritten on a recycling basis once the drive is full and in any event will not be held for more than 31 days.

1.5.3.2. Images stored on removable media such as CD will be erased or destroyed once the Purpose is no longer relevant. All digital recordings will be digitally water marked to maintain integrity.

1.5.4. University Records Policy

1.5.4.1. Images and recording logs will be held in accordance with the University Records Policy and Retention and Disposal Schedule. A copy of the Schedule is available online at: http://isd.ulster.ac.uk/__data/assets/pdf_file/0015/1554/retention-and-disposal-schedule.pdf

1.5.4.2. Recorded media no longer in use will be confidentially destroyed.

1.5.5. Access to and Disclosures of Images to Third Parties

1.5.5.1 Images recorded on CCTV will be restricted and carefully controlled in order to ensure that the rights of the individual are maintained and also that they can be used as evidence if required. Images can only be disclosed in accordance with the Purposes for which the information was originally collected and in accordance with the Notification with the Office of the Information Commissioner (as required by the DPA). A copy of the University's Notification is available by on the website of the Information Commissioner at: http://ico.org.uk/ESDWebPages/DoSearch

1.5.5.2. Access to images will be restricted to those staff that need to have access for the Purposes.

1.5.5.3. All access to CCTV images recorded on any media will be registered.

1.5.5.4. Disclosures to third parties will only be made in accordance with the Purposes and will be limited to;

(a) police and other law enforcement agencies where the images recorded could assist in a specific crime enquiry and/or the prevention of terrorism and disorder*;

(b) prosecution agencies;

(c) relevant legal representatives;

(d) people whose images have been recorded and are still retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings);

(e) in exceptional cases, to others to assist in identification of victim, witness or perpetrator in relation to a criminal incident; and

(f) members of staff involved with University disciplinary processes.

For the avoidance of doubt, recorded CCTV images shall not be made available to anyone other than those persons set out above.

The Data Protection Co-ordinator, or their designated agent, *are the only staff that can authorise disclosure of information to the police or other law enforcement agencies.*

1.6. Data Subjects Access Rights

1.6.1. The DPA gives individuals the right to access personal information about themselves, which includes CCTV images.

1.6.2. All requests for access to CCTV images should be made in writing to the University's Data Protection Co-ordinator, c/o Mr Eamon Mullan, University Secretary, Ulster University, Cromore Road, Coleraine BT52 1SA or by email at e.mullan@ulster.ac.uk. All requests will be treated as a Subject Access Request under the DPA. Any requests need to include the date, time, and location where the CCTV image was recorded and may require further information to identify the individual. A £10 fee will be payable to the University. The University will respond promptly and at the latest within 40 days of receiving the fee and sufficient information to identify the CCTV images. A copy of the University's Subject Access Request form and further information on the process is available online at: http://www.ulster.ac.uk/secretary/policyimplementation/dataprotection/sar_form.pdf. Hard copies of the form and information on the process is also available by contacting the individuals listed in Appendix 1 to this Policy.

1.6.3. Security staff will refer all such requests to the University's Data Protection Co-ordinator.

1.6.4. If the University cannot comply with a request under the DPA the reasons must be documented as to why not. The data subject must be advised in writing, giving the reason why the information cannot be released, where possible.

1.6.5. The manager responsible for the CCTV system will determine whether disclosure of the CCTV images would disclose third party information.

1.6.6. Where CCTV images reveal other individuals, the University must blur or disfigure the faces of those other individuals so that they are not recognisable.

1.6.7. In addition to the right of access, an individual also has the right to ask the University to stop processing personal data where this is likely to cause substantial and unwarranted damage to him or her. Any such requests should be submitted in writing to the University's Data Protection Co-ordinator. Upon receipt of such a request the University has 21 days in which to respond with its decision. All decisions should be documented and a record should be kept of all requests and the University's response to those requests.

1.6.8. A copy of the University's CCTV guidelines will be provided to anyone making a written request for it under the Freedom of Information Act 2000.

1.6.9. If there is any doubt about what information must be provided to enquirers, please contact the University's Data Protection Co-ordinator.

1.7 Responsibility for CCTV Systems

1.7.1. For systems operated by Facilities Services the overall responsibility lies with the Head of Facilities Services.

1.7.2. Day to day responsibility of each Campus is as follows:

Jordanstown:	Facilities Services Manager
Belfast:	Assistant Facilities Services Manager
Coleraine:	Head of Facilities Services
Magee:	Assistant Facilities Services Manager

1.8 Complaints

1.8.1. Complaints and enquiries about the operation of CCTV should be addressed to those having day-to-day responsibility, as listed above. Contact details are available upon request to the University's Director of Physical Resources on telephone no. 028 7012 4133.

1.8.2. Enquiries relating to the DPA should be referred to the University's Data Protection Co-ordinator.

1.8.3. If the individual is not satisfied with the response that he/she receives they should write in the first instance to the Head of Facilities Services who may in turn refer the matter to the University's Data Protection Co-ordinator.

1.9 Monitoring Compliance

The respective managers of relevant areas are to undertake occasional reviews with the University's Data Protection Co-ordinator to ensure updating of knowledge and compliance with the Policy and relevant legislation.

1.10 Compliance with this Policy

1.10.1. All employees (including temporary and contract staff) who are responsible for implementing, managing, operating or using the CCTV system must do so:

1.10.1.1. only as authorised and in accordance with this Policy;

1.10.1.2. with respect to those individuals who are being monitored; and

1.10.1.3. for the Purposes.

1.10.1.4. Any failure to comply with this Policy may be a disciplinary offence which could result in dismissal. Negligent or deliberate breaches could result in criminal liability for you personally.

APPENDIX 1

CONTACT DETAILS

Data Protection Co-ordinator	Mr Eamon Mullan Telephone No: (028) 7012 4533 E-mail: e.mullan@ulster.ac.uk
Equality and Legal Manager	Ms Angela Getty Telephone No: (028) 9036 8869 E-mail: ak.getty@ulster.ac.uk
Policy Co-ordinator	Ms Elinor Byrden Telephone No: (028) 7012 3354 E-mail: e.byrden@ulster.ac.uk