Closed Circuit Television (CCTV) Policy

(V 1.00)

This document describes the processes and measures which the University will use to manage and secure its installation and operations of its chosen CCTV system(s).

Table of Contents

Contents

1. Policy Statement

Plymouth Marjon University uses Closed Circuit Television (CCTV) to provide a safe and secure environment for students, staff and visitors and to protect University property. During the course of our activities, we will use Closed Circuit Television (CCTV) systems which may collect, store and process personal information about our employees, students and other third parties. We recognise the need to treat this in an appropriate and lawful manner.

Any breach of this policy will be taken seriously and may result in disciplinary action. Plymouth Marjon University's CCTV systems will at all times operate fairly, within the law, and only for the purposes for which they were established or are subsequently agreed in accordance with this policy.

2. About this policy

This document sets out the accepted use and management of the CCTV equipment and images to ensure the University complies with the relevant legislation. CCTV digital images, if they show a recognisable person, are considered as personal data.

Breach of this policy may be dealt with under our disciplinary procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal. Individuals breaching data protection requirements may also face personal criminal prosecution.

The Data Protection Officer is responsible for ensuring compliance with and with this policy.

3. Application of Data Protection Legislation

Where images of living, identifiable individuals are deliberately recorded, this is likely to comprise those individuals' personal data. The collection, use and storage of personal data are governed by data protection law. Plymouth Marjon University is registered with the Information Commissioner as a Data Controller operating CCTV.

Data subjects' rights, including a right of access to personal data, (in accordance with article 15 of GDPR), will be respected where recordings are confirmed to comprise personal data. The CCTV system will be operated with due regard for privacy of the individual and in accordance with Article 8 of the European Convention on Human Rights (ECHR) i.e. an individual's right to privacy.

The CCTV system is fundamentally an overt system, operated by the University and is used within the confines of the recognised Plymouth Marjon University campus. The CCTV system's existence and presence will be declared as in section 4 of this document.

Any changes to the purposes for which the CCTV system is operated will require the prior approval of the CCTV system owner, in consultation with the Chief Operating Officer and will be published internally as part of this Code at Section 3.

4. Purpose of CCTV

The system is intended to provide an increased level of security in the University environment for the benefit of those who study, work, live in or visit the campus.

The CCTV system will be used to respond to the following legitimate aims / key objectives, which will be subject to bi-annual review or sooner if required:

- assist in the prevention and detection of crime;
- facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order;
- help ensure public safety;
- assist with the identification of actions that may result in disciplinary proceedings against staff or students;
- provide and operate the system in a manner that is consistent with respect for individual's privacy;

As community confidence in the system is essential, all cameras will be operational. An appropriate maintenance programme will be established.

5. Use of CCTV

5.1 Cameras shall be installed in such a manner as not to overlook private domestic areas.

5.2 Cameras shall not be hidden from view and signs will be prominently displayed in the immediate locality of the cameras where possible and on entry to zones where CCTV is in operation i.e. entrance to a building.

5.3 The University will ensure staff, students and visitors are made aware of the presence of the system by appropriate signage. Signs will be prominently placed at strategic points and at entrances and exits of the campus. The signage will set out the purposes for processing CCTV images indicate:

- The presence of monitoring and recording.
- The ownership of the system.
- Contact telephone number.

6. Access to images & retention

Recorded images are held centrally and access to these recordings will be restricted to those staff who need to have access in accordance with the purposes of the system. For operational purposes, and in accordance with the stated purposes of the system, only designated Security staff, trained in their duties, shall have access to live CCTV footage.

Viewing of recorded images should take place in a restricted area to which other employees will not have access while viewing is occurring. Images retained for evidence should be securely stored.

7. Access to recordings

For operational purposes and in accordance with the stated purposes of the system, only designated Security staff shall have primary access to all CCTV recordings**.**

Disclosure of images from the CCTV system must be controlled and consistent with the purpose for which the system was established.

Disclosure of information to third parties will be made in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)
- In exceptional cases, to others to assist in identification of a victim, witness or perpetrator in relation to a criminal incident
- Members of staff involved with University disciplinary processes.
- Contractors working on University property

Only Senior Management can authorise disclosure of information to the police or other law enforcement agencies.

All requests for disclosure must be documented, for external parties, this should be done via the Subject Access Request form. For Internal requests, the form (Appendix A) should be completed and sent to the CCTV system owner for consideration.
If disclosure is denied the reason should be recorded.

8. Retention of Recorded Materials and Disposal

CCTV recordings and other materials produced from them shall be retained for thirty-one days unless an incident is recorded which requires further investigation either by the university security team, the police or another external body with prosecuting powers. In the latter case, recordings are deleted once shared with the relevant authority.

APPENDIX

Appendix A: Data Protection Principles.

- Processing shall be taken to mean all operations including obtaining, recording, storing, analyzing or converting into other formats.
- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and where necessary kept up to date;
- Kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Processed in a manner that ensures appropriate security of the personal data including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Appendix B: Request to view CCTV images

Name of requestor	
Reason for request	
Location, Date and start & finish times for requested recordings	
Approved by – (one from below) • Chief Operating Officer • POD Director • PVC (Student Success)	

Copy of completed request (whether approved or rejected) to be sent to CCTV system owner for logging.

Appendix C: Viewing Procedure

- Once approval has been given the requested recording will be made available to the requestor on a read-only basis for a period of no more than 5 days. After this time the recordings will be held for a further calendar month before deletion.

- The requestor must view the recordings in a secure environment and take care to ensure that viewing is restricted to the relevant audience.

- No copies of the recording are to be made by the requestor.

- The requestor may ask for copies of all or portions of the recordings to be kept pending further action which itself must be approved.

Document title:	CCTV Policy
Document reference:	CCTV Policy
Author:	Pete Waterfield
Document date:	11 August 2023
Confidential?	No
Document status:	Live
Document Version:	V1.00