# CODE OF PRACTICE
# FOR THE MANAGEMENT & OPERATION OF CCTV

| | |
|---|---|
| CATEGORY | **Finance & Estates** |
| POLICY OWNER | **Facilities Services Manager** |
| DATE & VERSION | **04-12-2023 - Version 3** |
| APPROVED BY | **Finance & Estates Committee** |
| REVIEW FREQUENCY | **Annual** |

**Contents**

## 1. Policy Purpose

The purpose of this Code of Practice is to regulate the management, operation and use of the closed circuit television (CCTV) system at UWC Atlantic (the College). This Code of Practice will be subject to review, to include consultation as appropriate with interested parties and follows the guidelines as per the policy statement below.

## 2. Policy Statement

The CCTV Scheme meets the requirements of the Information Commissioners Office (ICO), the Data Protection Act (2018), UK GDPR and will seek to comply with the requirements of both the Data Protection Act (2018) and the Surveillance Camera Code of Practice as published by the Home Office and updated in 2021.

## *3.* Policy Implementation

### 3.1 Operation of the System

The CCTV systems will be monitored by the Welcome Team and administered and managed by the ICT Team in accordance with the values and objectives expressed in the code. The day-to-day monitoring will be the delegated responsibility of the Welcome Team during normal working hours, out of hours and at weekends. The CCTV system is intended to operate 24 hours every day, recording all activity and the systems will generally overwrite the recorded data every 30 days or sooner.

### 3.2 Control and Liaison

The Head of ICT is the designated system administrator and will ensure that the system is periodically checked to confirm the efficiency of the system and, in particular, that the equipment is properly recording and that cameras are functional. Servicing and maintenance will be undertaken by either directly employed staff of the College or a specialised external contractor engaged by the Head of ICT.

### 3.3 Assessment of the Scheme and Code of Practice

The College's senior management or system administrator may carry out performance monitoring, including random operating checks.

### 3.4 Monitoring Procedures

Camera surveillance will as far as is reasonably practicable be maintained at all times and active footage recorded and held on tape or hard drive for no less than 7 days and generally no more than 30 days.

### 3.5 Viewing/Release of Images/Sequences

Images are viewed daily by the Welcome Team and images may be used as part of an internal investigation process involving potential breaches in the college student Behaviour Policy.

As images collected by the scheme may contain personal data, under the data protection act, the viewing/release of images outside of employees involved in the student disciplinary process at the College, will be regulated and monitored. Appendix 1 details the procedure to ensure both compliance with legislation and also help maintain and preserve the integrity of any images or image sequences provided as evidence.

### 3.6 Breaches of the code (including breaches of security)

The Director of Operations & Sustainability or the Data Protection Officer (DPO) will initially investigate any breach of the Code of Practice by College staff. Any serious breach of the Code of Practice will be subject to the terms of disciplinary procedures already in place.

### 3.7 Complaints

Any complaints received in respect of the operation of the CCTV scheme will be recorded in a complaints log and investigated in accordance with Section 9 of this Code, any complaints about the College's CCTV system should be addressed to the Data Protection Officer.

### 3.8 Access by the Data Subject

The Data Protection Act (2018) provides Data Subjects (individuals to whom "personal data" relate) with a right to access data held about them, including that obtained by CCTV. Data Subject Access Requests (SARs) should be made to david.emery@uwcatlantic.org, the Director of Operations & Sustainability as the Designated Data Controller. The Data Controller has the right to seek the advice of the Data Protection Officer, before responding to a SAR, as certain exemptions may be relevant.

### 3.9 Public information

Copies of this Code of Practice will be available to the public via the College website or upon request from the Compliance and Risk Manager.

### 3.10 Summary of Key Points

- This Code of Practice will be reviewed on a regular basis, not exceeding 24 months or when changes in legislation or guidance require it.
- The CCTV systems are leased / owned and operated by the College.
- Liaison meetings may be held with the Police and other groups or bodies.
- Recorded images will be properly indexed, stored and destroyed after appropriate use.
- Recorded images may only be viewed by authorised College staff as identified in this code or the Police and other external agencies or bodies upon request and approval.
- Images/Sequences required as evidence will be properly recorded, witnessed and packaged before copies are released to the police.
- Images/Sequences will not be made available to the media or for commercial or entertainment purposes, but only in support of the detection of crime as advised by the Police.
- The Director of Operations & Sustainability as the Designated Data Controller, will conduct the initial investigation into any breaches of this code.
- Breaches of the code and necessary actions will be reported to the Director of Operations & Sustainability as the Designated Data Controller or to the Principal.

## 4. Related Information

4.1 Relevant Policies

- Data Protection Policy
- Data Retention and Deletion Policy

## *5.* Policy Measurement and Reporting

The Code of Practice for the Management & Operation of CCTV Policy is reviewed annually by the Finance & Estates Committee of the Board and the Director of Operations & Sustainability as part of the annual review cycle and as part of the whole College development plan. Part of this review process will consider to what extent the policy is being used as an active working document.

The policy is communicated to the school community electronically on ***Every*** and is available on the UWCA website.

## Appendices

### Appendix 1 - CCTV system outline

The CCTV system at UWC Atlantic comprises a mixture of fixed or dome cameras located within buildings or at various locations around the site and configured as a single system. All cameras are connected via the College IP Network to a Virtual Digital Video Recorder managed and administered by the ICT Department. The system is web enabled and password protected and monitored operationally by The Welcome Team. The College owns or leases the CCTV systems.

The College will treat the system and all information, documents and recordings obtained and used as data protected by the Act. Cameras will be used to monitor activities within the College and the grounds to identify activity actually occurring, anticipated or perceived, and for the purpose of securing the safety and wellbeing of the College's students, staff, residents, visitors and other authorised users of the site.

Cameras are positioned to ensure they do not focus on private homes, gardens and other areas of private property and moveable PTZ cameras will at no time be positioned to focus on private homes, gardens or other areas of private or tenanted property.

Materials or knowledge secured as a result of CCTV use will not be used for any commercial purpose. Digital footage taken with the systems will only be released for use in the investigation of a specific crime in response to a written request from the police or other regulated organisations or companies who have a legal right to access such data.

Recorded camera footage will never be used or released for purposes of entertainment. The planning and system design has endeavoured to ensure that the CCTV Scheme gives maximum effectiveness and efficiency within available means, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at access points to the site and where possible to areas covered by the College's CCTV systems.

**Appendix 2 - Objectives of use of the CCTV system.**

The objectives of the College's use of CCTV are:

a) To increase the personal safety of students, staff, site residents and other site users and visitors, and to reduce the fear of crime

b) To support reporting on student behaviour not in keeping with the college behaviour policy (e.g. students out of houses following check in and before agreed times in the morning).

c) To protect the College's buildings, grounds and assets

d) To support the Police in a bid to deter and detect crime

e) To assist in identifying, apprehending and potentially prosecuting offenders

f) To assist in managing the College and reducing anti-social behaviour

g) To assist in managing vehicular movement around the site

**Appendix 3 - Viewing/Release of Images/Sequences**

a) A central register will be maintained of all requests for the release/viewing of images from the CCTV scheme (T:Drive//CCTVLog). This register will be managed by the ICT Team. The register will detail the date of the request, the requestor's name and organisation, the reason for the request, the date, time and duration of the sequence, the request outcome and the name of the approval decision maker.

b) Viewing of images or sequences by the Police or any external organisation, company or individual must be recorded in writing and entered in the register. Requests by the Police or others can be authorised under the Data Protection Act (2018). Should footage be required as evidence, a copy may be released to the Police, upon the verification of the request through a crime reference number and any subsequent identity checks.

c) Images or image sequences will only be released to the Police on the clear understanding that they remain the property of the College and are to be treated in accordance with this code. The College also retains the right to refuse permission for the Police or other

organisations, companies or individuals to pass to any other person the footage or any part of the information contained thereon save for occasions when a Court instructs said release.

d) Images or image sequences approved for release will be provided on transportable media, which must be identified by a unique reference number which is to be recorded in the register.

e) Images provided for evidential purposes must be sealed, witnessed and signed by the member of staff responsible for the recording, dated and stored in a secure evidence store or archive.

f) Applications received from outside bodies (e.g. solicitors) to view or release footage stored digitally will be referred to the Director of Operations & Sustainability as the Designated Data Controller and the Leadership Team. In these circumstances images will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, or in response to a Court Order.