

## CCTV (Closed Circuit Television) Policy

This document sets out the policy for Management and Operations of CCTV systems at the Penryn and Falmouth campuses.

<b>Organisation(s):</b>	FX Plus Falmouth University University of Exeter Students Union
<b>Applies to:</b>	Staff, Students, Applicants, Visitors, Contractors
<b>Required Consultees:</b>	Senior Executive Team
<b>Approved by:</b>	Senior Executive Team
<b>Date approved:</b>	27 July 2023
<b>Review date:</b>	27 July 2026

# CCTV Policy

---

This document sets out the policy to validate the roles and responsibilities of the system owners and the functions within and to ensure that all CCTV monitoring, recording and data distribution carried out by FX Plus is carried out in accordance with the Data Protection Act 2018, the Protection of Freedoms Act 2012 and the Human Rights Act 1998, as well as ensuring best practice and advice from the Surveillance Commissioner.

## 1. Purpose

1.1 The purpose of CCTV installations are:

- i. The protection of staff, students, visitors, and the assets of the Universities and Falmouth Exeter Plus;
- ii. The prevention and investigation of Criminal or Health and Safety incidents;
- iii. The apprehension and prosecution of offenders (including the use of images/data as evidence in criminal / civil proceedings);
- iv. The monitoring of the security of premises.

## 2. Scope

2.1 The principles of this policy are:

- i. that individuals' rights are respected and protected;
- ii. that the installations are operated fairly and within the law;
- iii. that the CCTV system is operated for the purposes for which it was set up;
- iv. that the recorded material/data stored is fairly and lawfully processed;
- v. that recorded material/data is adequate, relevant and not excessive for the purposes;
- vi. that recorded material/data is accurate, securely stored, and not kept for longer than is necessary.

## 3. Related information

3.1 Information can be found on the Falmouth Exeter Plus Intranet here [CCTV Data Protection Impact Assessment \(sharepoint.com\)](#)

## 4. Key Definitions

CCTV: Closed Circuit Television  
BWV: Body Worn Video  
DPA: Data Protection Act 2018

## 5. Operation of CCTV system

5.1 The CCTV system will be monitored to observe the campuses and areas under surveillance in order to identify incidents requiring a response.

- 5.2 Any response should be proportionate to the incident being witnessed.
- 5.3 Images are recorded centrally on servers located securely at Penryn Campus and are viewable in Safety and Support Team areas.
- 5.4 Additional staff may be authorised by the Head of Safety and Support to monitor cameras sited within their own areas of responsibility on a view only basis.
- 5.5 All staff viewing CCTV must be aware of their responsibilities outlined by this policy.

## **6. CCTV Access**

- 6.1 There are several levels of CCTV user access within FX Plus and these are dictated by their need to view and process data from the CCTV System. The CCTV users are categorised as:
  - 6.1.1 Limited Operator: Their system access will allow the viewing and reviewing of CCTV footage relevant and proportional for their job role and responsibilities (such as Halls Officers may view Halls CCTV camera footage).
  - 6.1.2 Full Operator: Their system access will allow the downloading, viewing and reviewing of CCTV footage relevant and proportional for their job role and responsibilities. Downloads are only to be carried out in accordance with the FX Plus CCTV Policy. They will also be able to control the pan, tilt and zoom of cameras in real time operation.
  - 6.1.3 Administrator: They will have full access to the CCTV System, allowing them to download, view and review footage as well as control cameras and assign access levels to Operators. The Administrators will be restricted to being: Head of Safety and Support, Safety and Support Operations Manager, Safety and Support Duty Managers and the Security Compliance and Safety Officer.

## **7. Retention of Images**

- 7.1 Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 30 days from the date of recording. Images will be automatically overwritten after this point.
- 7.2 Where an image is required to be held in excess of the retention period referred to in the above paragraph the Head of Safety and Support, Data Protection Officer or their nominated deputy, will be responsible for authorising such a request and must record why the retention period has been extended and provide an expected destruction/overwrite date.
- 7.3 At the end of their useful life all images stored in whatever format will be erased securely.
- 7.4 All still photographs and hard copy prints also will be securely disposed of as confidential waste.

## **8. Disclosure of Images**

- 8.1 Third parties who wish to have a copy of CCTV images do not necessarily have a right of access to images under the DPA 2018, and care must be taken when complying with such requests to ensure that neither the DPA 2018 or the CCTV Policy are breached.
- 8.2 Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system, via the Data Protection Officer and, is limited to the following:
  - 8.2.1 Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry, and at the university's discretion).
  - 8.2.2 Prosecution agencies.
  - 8.2.3 Appropriate members of university staff in the course of staff or student disciplinary proceedings (including prospective proceedings) to ensure compliance with the university's regulations and policies.
  - 8.2.4 Representatives of Exeter and/or Falmouth Universities
  - 8.2.5 People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries).
  - 8.2.6 Organisations with which FX Plus have a Data Sharing Agreement with that enables them to have access to CCTV images.
- 8.3 All third party requests for access to a copy of video footage should be made in writing to the Data Protection Officer.
- 8.4 If a law enforcement or prosecution agency is requesting access they should make a request under Section 29 of the Data Protection Act 1998, where this is done outside normal working hours the Duty Manager may release the footage but must inform the Head of Security and Data Protection Officer that this has been done.
- 8.5 Whenever CCTV data has been disclosed to a third party it must be logged as to who has accessed it, when (date/time) it was accessed, what organisation they are from, details of what was viewed and why.
- 8.6 Any digital media containing CCTV footage that has been disclosed must be signed for and the person receiving that data must be given a statement outlining their Data Protection responsibilities.
- 8.7 Individuals (and organisations on behalf of individuals) under DPA 2018 have the right to access personal data, including CCTV footage of themselves. Any such requests must be made to the Data Protection Controller who will process this request. Note that whilst individuals have a right to view footage of themselves, FX Plus must also ensure that Data Protection of others who are also visible on the footage.

## 9. Accountability and Responsibility

- 9.1 The CCTV System is owned by FX Plus.
- 9.2 The Director of Residences and Facilities is accountable for the overall management of CCTV systems.
- 9.3 The Head of Safety and Support and their immediate deputies are responsible for approving access rights to CCTV footage for FX Plus staff and designated CCTV contractors.
- 9.4 Anyone with rights to access CCTV data is responsible for ensuring it is processed lawfully and in line with this Policy.
- 9.5 The Head of Safety and Support is responsible for auditing compliance against the CCTV policy.
- 9.6 The Data Protection Officer is responsible for advising on compliance with the DPA and other legislation.
- 9.7 Where new CCTV cameras are to be installed or existing cameras recited, the Head of Safety and Support and the Data Protection Officer’s approval must be sought and recorded.

## 10. Equality Impact Assessment

*An Equality Impact Assessment is the process of considering the potential impact of a policy (referred to as an activity) on different groups of people according to their protected characteristics. It is unlawful to discriminate against people on the grounds of one or more of the protected characteristics detailed in 2010 Equality Act.*

*Does the policy or activity have a notable adverse impact on people according to their status in relation to the following protected characteristics?*

Characteristic	Negative impact –Y/N
Sex	N
Race	N
Age	N
Marriage / civil partnership	N
Disability	N
Gender reassignment	N
Sexual orientation	N
Pregnancy / maternity	N
Religion / belief	N

*If you have answered yes to any of the above, it is advised that an [Equality Analysis Form](#) is completed. The above table will be removed prior to publishing the Policy.*

- 10.1 The author has confirmed whether an Equality Impact Assessment is required and confirms that:
  - An Equality Impact Assessment is **not required**.
  - An Equality Impact Assessment **is required and has been completed**.

## 11. Contact for Further Information

- 11.1 Head of Safety and Support