

Information Governance

CCTV Policy

A review of this policy will be undertaken by the Information Governance Lead annually or more frequently as required, and will be authorised by the Information Governance Board for approval by the Senior Executive Team.

Title	CCTV Policy	
Description	Policy defining FX Plus approach to surveillance cameras	
Created By	Greensmith, Rob	
Document #	IGP012	
Date Created	15/10/2019	
Maintained By	Information Governance	
Review due date	15/10/2021	
Approval by Information Governance Board		
Approval by Senior Executive Team	15/10/2019	

Purpose

In order to operate legally and effectively, the FX Plus must operate its CCTV systems in line with the General Data Protection Act (GDPR), the Data Protection Act 2018 (and if the UK leaves the EU, the UK GDPR as implemented), the Surveillance Commissioner's Code of Practice 2013, the Protection of Freedoms Act 2012 and the Human Rights Act 1998, and to ensure best practice and advice supplied by the Surveillance Commissioner and the Information Commissioner's Office. FX Plus is registered with the Information Commissioner's Office and the registration number is Z8629765.

Scope

This policy applies to all members of staff of Falmouth Exeter Plus ("FX Plus"), and their subsidiary commercial services, including, but not limited to Cornwall Plus, the Sports Centre and the Nursery, staff and students from Falmouth University and the University of Exeter located on Penryn and Falmouth Campuses, and associated contractors operating on either campus.

Policy Statement

The purpose of the CCTV System is for the prevention, reduction and detection of crime and to ensure the safety of campus users and this policy defines how FX Plus will do this in a legal and ethical manner whilst still maintaining operational effectiveness.

Implementation

FX Plus own and operate CCTV systems at Penryn Campus, Falmouth Campus and Glasney Student Village and as such are the data controller for images produced, retained and distributed from the CCTV System.

Purpose of CCTV System

The principle purpose of the CCTV System is for the prevention, reduction and detection of crime and to ensure the safety of campus users, traffic management including reading number plates for the purpose of barrier operation as well as enforcing the Parking Policy where required. CCTV images may also be used for the investigation of suspected breaches in FX Plus, Falmouth University and University of Exeter policies and regulations, including staff and student disciplinary offences.

Operation of CCTV System

The CCTV system will be monitored to observe the campuses and areas under surveillance in order to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.

Images are recorded centrally on servers located securely at Penryn Campus and are viewable in Security Service areas by all Security staff. Additional staff may be authorised by the Head of Security to monitor cameras sited within their own areas of responsibility on a

view only basis. All staff viewing CCTV must be aware of their responsibilities outlined by this policy. In areas of surveillance, signs will be displayed prominently to inform employees that CCTV is in use. If workers access the relevant areas, their images will be captured on CCTV.

CCTV Access

All users must have individual log ins for the CCTV system, shared usernames and passwords are not to be used. 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:

Limited Operator: Allows 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).

Full Operator: Allows 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 Operations Procedure. Full operators will also be able to control the pan, tilt and zoom of cameras in real time operation.

Administrator: Allows full access to the CCTV System, allowing 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 Security, Security Systems Advisor and the Security Operations Manager.

Retention of Images

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.

Where an image is required to be held in excess of the retention period referred to in the above paragraph the Head of Security, 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.

At the end of their useful life all images stored in whatever format will be erased securely and permanently and where in physical form for example tapes or discs, disposed of as confidential waste. All still photographs and hard copy prints also will be securely disposed of as confidential waste.

Disclosure of Images

Third parties who wish to have a copy of CCTV images do not necessarily have a right of access to images under the GDPR, and care must be taken when complying with such requests to ensure that neither the GDPR or the CCTV Policy are breached.

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

- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry, and at the university's discretion).
- Prosecution agencies.

- Appropriate members of university staff (such as Human Resources and the Student Conduct, Complaints and Appeals team) in the course of staff or student disciplinary proceedings (including prospective proceedings) to ensure compliance with the university's regulations and policies.
- Representatives of Exeter and/or Falmouth Universities
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries).
- Organisations with which FX Plus have a Data Sharing Agreement with that enables them to have access to CCTV images.

All third party requests for access to a copy of video footage should be made in writing to the Data Protection Officer. If a law enforcement or prosecution agency is requesting access they will make a request under Schedule 2.1.2 of the Data Protection Act 2018, 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.

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. 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.

Individuals (and organisations on behalf of individuals) under GDPR and the Data Protection Act 2018, have the right to access personal data, including CCTV footage of themselves. Any such requests must be made to the Data Protection Officer who will process this request. Note that whilst individuals have a right to view footage of themselves, FX Plus must also protect the privacy of others who are also visible on the footage.

Limits on use of CCTV

Covert surveillance will not be undertaken by FX Plus under any circumstances.

CCTV will not be operated in toilets or changing rooms.

CCTV will not be operated in private offices unless there is a serious risk to health and safety. CCTV will be used in this way only where it is the most proportionate means of achieving the aim in the circumstances.

All cameras in use across the FX Plus managed estate will be identifiable and appropriate signage will be installed across the campuses operating under FX Plus jurisdiction.

Accountability and Responsibility

The CCTV System is owned by FX Plus.

The Head of Security and their deputies are responsible for approving access rights to CCTV footage for FX Plus staff and designated contractors.

Anyone with rights to access CCTV data is responsible for ensuring it is processed lawfully and in line with this Policy.

The Head of Security is responsible for auditing compliance against the CCTV policy.

The Data Protection Officer is responsible for advising on compliance with the Data Protection Act 2018, GDPR and other legislation.

Where new CCTV cameras are to be installed or existing cameras repositioned, the Head of Security's approval must be sought and recorded.

Review Period

This policy will be reviewed every 2 years, or when required due to legislation change or established practice adjustments.

Glossary of Terms

CCTV System: System consisting of camera equipment, storage, monitoring and associated equipment for transmission and controlling purposes.

ANPR (Automatic Number Plate Recognition): A surveillance technology which uses optical character recognition on camera images to read a vehicle's number plate.