University of Birmingham School

CCTV Policy

March 2023

University of Birmingham School

CCTV Policy

Review Frequency	Every two years	**Review date**	March 2023
Governing Committee Responsible	Audit	**Next Due**	March 2025
Governor Approval (date)	22 March 2023	**Website**	Yes
Staff Responsible	C Townsend	**Date Produced**	

CCTV POLICY

Introduction

The School recognises that CCTV systems can be privacy intrusive.

Review of this policy shall be repeated regularly and whenever new equipment is introduced a review will be conducted and a risk assessment put in place. We aim to conduct reviews no later than every two years.

Objectives

The purpose of the CCTV system is to assist the School in reaching these objectives:

(a) To protect pupils, students, staff and visitors against harm to their person and/or property.

(b) To increase a sense of personal safety and reduce the fear of crime.

(c) To protect the School buildings and assets.

(d) To support the police in preventing and detecting crime.

(e) To assist in identifying, apprehending and prosecuting offenders.

(f) To assist in establishing the cause of accidents and other adverse incidents and prevent reoccurrence

(g) To assist in managing the School.

Purpose of the Policy

The purpose of this Policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at the School.

Statement of Intent

The CCTV system will seek to comply with the requirements both of the Data Protection Act and the most recent Commissioner's Code of Practice.

The School will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency 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 will be clearly visible on the site.

Recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated. In the absence of a compelling need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than is absolutely necessary.

System Management

Access to the CCTV system and data shall be password protected.

The CCTV system will be administered and managed by the School's Facilities Manager who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager the system will be managed by one of the Facilities Team under the instruction of the School Business Leader.

The system and the data collected will only be available to the Systems Manager, their replacement and appropriate members of the senior leadership team as determined by the Principal.

The CCTV system is designed to be in operation 24 hours a day, though the School does not guarantee that it will be working during these hours.

The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.

Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by proving clear, usable images.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those mentioned above, requests access to the CCTV data or system, the System Manager must satisfy himself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists access will be refused. This may be managed under the principles of a subject access request (SAR) and the School may seek advice from its Data Protection Officer in order to secure compliance with acceptable protocols and data sharing under GDPR.

Downloading Captured Data onto Other Media

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any download media used to record events from the hard drive must be prepared in accordance with the following procedures: -

(a) Each download media must be identified by a unique mark.

(b) Before use, each download media must be cleaned of any previous recording.

(c) The System Manager will register the date and time of download media insertion, including its reference.

(d) Download media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a download media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.

(e) If download media is archived the reference must be noted.

Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his replacement and the Principal and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable if possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any download media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the download media (and any images contained thereon) remains the property of the School, and download media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The School also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the School to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until they are needed by the police.

Applications received from outside bodies (e.g. solicitors or parents) to view or release images will be referred to the School's Data Protection Officer and a decision made by a senior leader of the School in consultation with the School's data protection officer.

Retention of CCTV Data

Whilst the Information Commissioner's Office stipulates neither minimum nor maximum periods for CCTV image storage (retention) the School will be guided by the GDPR principle that data should be retained for a period no longer than necessary with reference to the intent laid out in this policy. The School's current CCTV system routinely stores material for no longer than 30 days. In any event, CCTV imagery and recordings, including where transferred to other media or devices, will be retained for a period no longer than three calendar months from the date the data was captured by CCTV.

Complaints about the use of CCTV

Any complaints in relation to the School's CCTV system should be addressed to the School Business Leader, who may in turn delegate matters to the Director of Information and Systems at the School.

Request for Access by a Data Subject

The Data Protection Act provides Data Subjects – those whose image have been captured by the CCTV system and can be identified – with a right to data held about themselves, including those obtained by CCTV. Requests for such data should be made to the School Business Leader in the first instance.

Public Information

Copies of this policy will be available to the public from the School office, and are accessible via the School's website.

Policy Review and Monitoring

This policy will be reviewed biennially by the Audit Committee of Governors.