SANDWELL ACADEMY

CCTV Policy

September 2026

Policy Title:	Use of recorded media (CCTV etc)
Policy Reference:	SA / Staff
Description:	This document offers guidelines for students, parents and staff as to how the Academy will use recorded media
Status:	
Category:	Academy
Contact:	Name: Daljeet Kangh Title: Director of ICT Email : dkangh@sandwellacademy.com
Version:	V1.6
Other relevant SA polices:	
Adopted by the Governing Board on:	Not applicable
Date for Review:	July 2027

Change Record		
Version	**Date**	**Description**
1.1	**July 2021**	**Annual Review**
1.2	**July 2022**	**Annual Review**
1.3	**July 2023**	**Annual Review**
1.4	**July 2024**	**Annual Review**
1.5	**July 2025**	**Annual Review**

1.6	**July 2026**	**Annual Review**

Contents Page

Table of Contents

Contents Page 3
INTRODUCTION 4
DATA PROTECTION ACT & CCTV STANDARDS 4
Code of Practice 5
Breaches of the code 5

INTRODUCTION

The purpose of this policy is to regulate the management, operation and use of the CCTV system at Sandwell Academy.

Objectives of the CCTV:

- To increase personal safety of staff, students and visitors and reduce the fear of crime (Safeguarding arrangements).
- To protect the Academy building and their assets.
- To support the Police in a bid to deter and detect crime.
- To assist in identifying, apprehending and prosecuting offenders.
- To protect members of the public and private property.
- To assist in managing the Academy and to assist in the quality assurance of teaching and learning.

DATA PROTECTION ACT & CCTV STANDARDS

Sandwell Academy has chosen to use CCTV (Closed circuit television) in selected areas across the Academy including all external entrances and identified areas within the building. GDPR, Regulation of Investigatory Powers Act 2000 (RIPA) and CCTV Code of Practice issued by the Information Commissioner explains how CCTV systems should be used, so that Academies and individuals can enjoy security and safety whilst ensuring that individual rights are upheld. Sandwell Academy complies with the Code and adopts good standards of practice which helps towards realising this objective.

Use of CCTV can be covered by a number of Acts including the GDPR, the Human Rights Act and the Regulation of Investigatory Powers Act (RIPA). Failure to comply with these Acts or the related codes would cause the Academy to be in breach of the Law, render any evidence as inadmissible or carry penalties for the Academy, as the CCTV user, or individual members of staff.

The live footage from the CCTV system is displayed in the Gate House, where it is monitored by the Security staff. This provides a layer of proactive monitoring of external door access to enhance safeguarding arrangements.

Key staff have been provided with the necessary induction in the use of the CCTV systems and only those members of staff have access to the recordings within the system.

The Academy has undertaken the following checklist to ensure that the CCTV system remains within the law and that images can be used for crime prevention.

- The Academy has specified that the CCTV cameras have been installed for the safeguarding of staff and students and for detection and prevention of vandalism across the Academy estate.
- Significant signage is found in prominent positions in all areas where CCTV cameras operate to inform staff, students and the general public that they are entering an area where their images are being recorded either as still or video footage.
- The Academy retains the right to be the data controller for all footage recorded through the use of its CCTV cameras.
- The equipment is sited so that it only monitors those spaces that are intended to be covered by the equipment.

- All operators (staff who operate and monitor CCTV) are aware of the purposes for which the scheme has been established.
- Operators are aware that they are only able to use the equipment in order to achieve the purposes for which it has been installed.
- The images are stored on a secure server the retention period is for 28 days approx. unless footage has been bookmarked and locked.

Code of Practice

- This CCTV Policy will be reviewed every two years.
- The CCTV system is owned and operated by the Academy.
- The footage may only be viewed in the presence of the authorised members of staff.

Breaches of the code

- Any breach of the code of Practice by the Academy will be initially investigated by the I.T Director and reported to the Headteacher, in order for them to take the appropriate disciplinary action.
- Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

The following do's and don'ts as advised as part of the Data Protection Policy and are adhered to by the Academy.

Do

- Ensure CCTV is the only viable option to achieve the stated purpose.
- Formally assess the appropriateness of and reasons for, using CCTV.
- Consult the relevant parties involved.
- Undertake regular reviews of both the use of the CCTV system and the procedures to ensure compliance with the law.
- Ensure that film / images are not kept for longer than necessary.
- Process (working with, using, passing on data) images in a lawful manner.
- Make certain there are procedures for dealing with police enquiries, i.e. access under the DPA or removal of evidence under Police and Criminal Evidence Act.

Don't

- Film areas that could amount to an infringement of personal privacy.
- Ignore subject access requests (an individual's written request to access information about themselves under the Data Protection Act). A person identifiable on CCTV images may be entitled to view the footage and may make a request to do so.
- Use CCTV footage for any other purpose other than what it was originally used for e.g. Prevention and detection of a crime.
- Use covert (i.e. where it is calculated to ensure that the persons are unaware) monitoring without seeking legal advice.
- Use inadequate equipment. Blurred or indistinct images could constitute as inadequate data, whilst poorly maintained equipment may not provide legally sound evidence.
- Disclose data to third parties, unless it is lawful to do so.
- Systematically monitor people by use of CCTV.