

## POLICY DOCUMENT

### 002: CCTV

**Access:** Unrestricted

**Publish to:** All Staff / All Pupils and School Website

**Status:** Non-statutory

**Approval level:** Finance & Resource Committee

Review Responsibility	Valid from	Valid to	Review date	Frequency of review	Signed off by
Business Manager	30-06-2022	30-06-2024	30-05-2024	2 Years	FR Committee 05-07-2022
Business Manager	28-06-2024	28-06-2026	28-05-2026	2 Years	FR Committee 02-07-2024

## **Closed Circuit Television (CCTV) Policy**

### **Contents**

1. Introduction .....	
2. Statement of Intent .....	
3. Siting the Cameras.....	
4. Covert Monitoring.....	
5. Storage and Retention of CCTV images.....	
6. Access to CCTV images.....	
7. Subject Access Requests (SAR) .....	
8. Access to and Disclosure of Images to Third Parties.....	
9. Complaints.....	

### **Appendix A Checklist**

### **Appendix B Signage**

### **Appendix C GDPR and the Data Protection Act 2018**

## **Introduction**

The Polygon School uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to school property.

The system comprises of fourteen static and one mobile camera covering a variety of locations external to the school building. The systems do not have sound recording capability. The CCTV system is owned and operated by the school and the deployment of which was determined by the school's leadership team. The CCTV is monitored centrally from the Medical Office located within the 'Staff Only' Area. It is also monitored via laptop software by the Head teacher, Deputy head teacher, Business Manager, Site Manager and Reception.

The use of CCTV, and the associated images are covered by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy outlines the school's use of CCTV and how it complies with the Act.

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained by the school data controller in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound. The CCTV is overseen by the Site Manager.

## **Statement of Intent**

The School complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The (ICO) CCTV Code of Practice is currently being reviewed, but once completed, it can be found at: <https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>

CCTV warning signs will be clearly and prominently placed at all external entrances to the school, including school exterior gates if coverage includes outdoor areas. The school will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

The planning and design has endeavoured to ensure that the Scheme 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.

## **Siting the Cameras**

Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.

The school will make every effort to position cameras so that their coverage is restricted to the external school premises.

CCTV are installed for external use only and will not be used in classrooms.

Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

### **Covert Monitoring**

The school may in exceptional circumstances set up covert monitoring. For example:

- Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances authorisation must be obtained from the Head teacher.

Covert monitoring must cease following completion of an investigation.

Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets

### **Storage and Retention of CCTV images**

Recorded data is retained for approximately two weeks. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded. All retained data will be stored securely. Access to CCTV images or access to recorded images will be restricted to those staff authorised to view them and will not be made more widely available.

### **Subject Access Requests (SAR)**

Individuals have the right to request access to CCTV footage relating to them under the Data Protection Act.

All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

The school will respond to requests within 40 calendar days of receiving the written request and fee. A fee of £100 may be charged per request at the school's discretion.

The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

### **Access to and Disclosure of Images to Third Parties**

There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).

Requests should be made in writing to the Headteacher.

The data may be used within the school's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

### **Complaints**

Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance. This policy will be reviewed and approved by the Finance Committee every two years, or earlier where there is a change in the applicable law affecting this Policy Guidance.

Further Information on CCTV and its use:

- CCTV Code of Practice (published by the Information Commissioners Office) <https://ico.org.uk/>
- Regulation of Investigatory Powers Act (RIPA) 2000
- General Data Protection Regulation (GDPR) and the Data Protection Act 2018

## **Appendix A – CCTV Signage**

It is a requirement of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the school
- The contact telephone number or address for enquiries

### **WARNING CCTV cameras in operation**

Images are being monitored and recorded for the purpose of preventing crime, anti-social behaviour and bullying, for the safety of staff and pupils and for the protection of the School and its property. This system will be in operation 24 hours a day, every day. These images may be passed to the Police. This scheme is controlled by The Polygon School. For more information contact the Site Manager on 023 8063 6776.

## **Appendix B – GDPR and the Data Protection Act 2018**

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018: Data Protection Principles states that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals.
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

**This is not a full explanation of the principles, for further information refer to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.**