CLOSED CIRCUIT TELEVSION (CCTV) SYSTEM POLICY

This policy is prescribed by The Good Shepherd Trust and all reference to 'the Trust' includes all Trust schools, the central team and subsidiary organisations.

Date adopted:	January 2021	Last reviewed:	25th January 2023
Review cycle:	Every 2 years or earlier	Is this policy statutory?	No
Approval:	Louisa Mason	Authors:	David Bird, Peter Coates
Local Approval:	Local Committee	Local Author:	Kate Harper-Cole

Revision record

Minor revisions should be recorded here when the policy is amended in light of changes to legislation or to correct errors. Significant changes or at the point of review should be recorded below and approved at the level indicated above.

Revision No.	Review Date	Revised by	Approved date	Comments
1	25.01.2023	Peter Coates	15 February 2023	Changes made to the layout of the CCTV policy – adding more depth to CCTV system overview and adding in links to policies. Additional sections added: monitoring of classroom Length of time recordings kept amended Complaint procedure SAR info Definitions and Statement of Intent
2				
3				

1. Introduction

1.1. Definitions

Surveillance: the act of watching a person or a place

CCTV: closed circuit television; video cameras used for surveillance

Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance

1.2. Legislation

Valley End School has in place a CCTV surveillance system 'the CCTV system' across its premises. This policy details the purpose, use and management if the CCTV system in the School and details the procedures to be followed in order to ensure that the School complies with relevant legislation and the current Information Commissioner's Office (ICO) Code of Practice.

The School will conform to the requirements of the Data Protection Act 2018 (DPA 2018), the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000 , the Protection of Freedoms Act 2012 and the Human Rights Act 1998.

Although not a relevant authority, the School will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and in particular the 12 guiding principles contained therein.

This policy is based upon guidance issued by the Information Commissioner's Office, 'In the picture: A data protection code of practice for surveillance cameras and personal information' ('the Information Commissioner's Guidance').

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

1.3. **Statement of intent**

The purpose of the CCTV system is to:

- Make members of the school community feel safe
- Protect members of the school community from harm to themselves or to their property
- Deter criminality in the school
- Protect school assets and buildings
- Assist police to deter and detect crime
- Determine the cause of accidents
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defense of any litigation proceedings

The CCTV system will not be used to:

- Encroach on an individual's right to privacy
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- Follow particular individuals, unless there is an ongoing emergency incident occurring
- Pursue any other purposes than the ones stated above

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and UK GDPR.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

2. CCTV Systems Overview

The CCTV system is owned by Valley End School and managed by the School and its appointed agents. The data controller for CCTV images held Valley End School is the Good Shepherd Trust (GST). GST is registered with the Information Commissioner's Office (ICO). The registration number is ZA261347.

The Trust's Data Protection Officer is responsible for ensuring that GST complies with the Data Protection Law. The Data Protection Officer can be contacted on admin@goodshepherdtrust.org.uk or 01483 910210.

The CCTV operates to meet requirements of the Data Protection Act 2018 and the Information Commissioner's Guidance.

Valley End School's designated Data Protection Lead is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.

The Data Protection Lead is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.

The CCTV system is operational and capable of being monitored for 24 hours a day, every day of the year.

Any CCTV installation shall be subject to a Data Protection Impact Assessment. It will also comply with the policy and procedures within the document. The Data Protection Impact Assessment shall be appended to this policy and shared with the GST Data Protection Officer.

3. Purposes of the CCTV system

The principal purposes of the School's CCTV system are as follows:

- For the prevention, reduction, detection and investigation of crime and other incidents.
- To ensure the safety of staff, pupils, visitors and members pf the public.
- To assist in the investigation of suspected breaches of school regulations by staff or students.

The CCTV system will be used to observe the school's building and areas under surveillance to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.

The school seeks to operate its CCTV system in a manner that is consistent with respect for the individuals privacy.

4. Monitoring and Recording

Cameras are monitored within the school in a secure area.

Images are recorded and are viewable in the secure setting within the school. They can also be viewed on request by all CCTV trained staff, by SLT members and by the Head. Additional staff may be authorised by the Head or Deputy Head to monitor cameras on a view only basis to support trained staff e.g. in identifying specific children. Any viewings will be made by **2** people at all times.

A log shall be kept of requests to access recorded images by staff and whether any recorded images have been copied to support specific investigations. Information logged should include: Name of staff, time and date of viewing, time and date images reviewed, brief reason for viewing the content (e.g. incident in corridor) but should not contain names, whether any images have been copied and where they have been copied to.

The cameras installed shall provide images that are of suitable quality for the specified purposes for which they are installed, and all cameras are checked regularly to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.

All images recorded by the CCTV system remain the property and copyright of GST. The recorded images are stored within the school. Downloaded footage used in investigations is securely stored on a server, in accordance with the process outlined in the retention of images section.

If CCTV is used to monitor classrooms, it will not be used to carry out lesson observations.

5. Compliance with Data Protection Legislation

The School will comply with the General Data Protection Regulation (GDPR). Due regard will be given to the data protection principles contained within Article 5 of the GDPR which provide that personal data shall be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

All storage used for images, recorded or downloaded for investigations, must be in compliance with GDPR rules; on secure storage on premise or on cloud storage.

The existence of the School's CCTV system must be recorded in the Record of Data Processing Activities.

6. Location of the cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1).

Cameras are located in:

- Outside of the main entrance, known as the 'cottage door' which is the arched door to the original school house building.
- Outside of the double green doors, on Valley End Road, where all pupils enter the school each day.
- Outside of the external playground door which links to the Early Years Cloakroom corridor.
- Outside of the ramped fire exit overlooking the external gate and staff car park at the far end of school.

Cameras are not sited to focus on private residential areas. Where cameras overlook residential areas, privacy screening or software masking will be utilised.

Wherever cameras are installed appropriate signage is in place to warn members of the school community that they are under surveillance. The signage:

- Is placed at all pedestrian and vehicular entrances to inform staff, pupils, parents, visitors and members of the public that CCTV is in operation.
- Indicates that the system is managed by the School and a 24-hour contact number for the Security Control Centre is provided, if appropriate.

- Identifies the school as the operator of the CCTV system
- Identifies the school as the data controller
- Provides contact details for the school

Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

7. **Roles and responsibilities**

The headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified
- Ensure that the guidance set out in this policy is followed by all staff
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO in the use of the system and in data protection
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO and taken into account the result of a data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties

The GST Data Protection Officer (DPO) will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Train all staff to recognise a subject access request
- Deal with subject access requests in line with the Freedom of Information Act (2000)
- Monitor compliance with UK data protection law
- Advise on and assist the school with carrying out data protection impact assessments
- Act as a point of contact for communications from the Information Commissioner's Office
- Assist with data protection impact assessments
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Ensure footage is destroyed when it falls out of the retention period
- Ensure that the CCTV system is not infringing on any individual’s reasonable right to privacy in public spaces
- Carry out annual checks to determine whether footage is being stored accurately, and being deleted after the retention period

The School Data Protection Lead will:

- XXXXX School's designated Data Protection Lead is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.
- Ensure clearly visible signs are placed at all pedestrian and vehicular entrances to inform staff, pupils, parents, visitors and members of the public that CCTV is in operation.
- The Data Protection Lead is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.
- Keep accurate records of all data processing activities and make the records public on request
- Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information

The system manager will:

- Take care of the day-to-day maintenance and operation of the CCTV system
- Oversee the security of the CCTV system and footage
- Check the system for faults and security flaws termly
- Ensure the data and time stamps are accurate termly
- Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified
- Receive and consider requests for third-party access to CCTV footage

8. Operation of the CCTV system

The CCTV system will be operational 24 hours a day, 365 days a year.

The system is registered with the Information Commissioner's Office.

The system will not record audio.

Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.

9. Applications for disclosure of images

9.1. Applications by individual data subjects

Requests by individual data subjects for images relating to themselves "Subject Access Request" should be submitted in writing.

In order to locate the images on the School's system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.

Where the School is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual. Any decision to withhold the requested images must be referred to the Group's Data Protection Officer or his team as there are specific rules that must be adhered to when applying the exemptions contained in the Data Protection Act 2018.

9.2. Access to and disclosure of images to third parties

A request for images made by a third party should be made in writing.

In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation.

All unexpected requests for CCTV images by a third parties, including requests made by the police, should be referred to the School's Data Protection Lead in the first instance and if not available to the Group's Data Protection Officer or their team, who will advise on the application of any appropriate exemptions.

Where a suspicion of misconduct arises and at the formal request of the Investigating Officer or HR Manager/ Business Partner, the Head may provide access to CCTV images for use in staff disciplinary cases.

The Head may provide access to CCTV images to Investigating Officers when sought as evidence in relation to staff discipline cases.

A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

10. 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 (this does not include school holidays or weekends) from the date of recording. Images will be automatically overwritten after this point.

The automatic deletion of data after the defined retention period should be checked on a half termly basis. This should be logged on a half termly basis.

Where an image is required to be held in excess of the retention period referred to in section 6, the Head or their nominated deputy will be responsible for authorising such a request. A record of these stored images will be kept within the CCTV viewing log.

Images held in excess of their retention period will be reviewed on a three-monthly basis and any not required for evidential purposes will be deleted. The CCTV monitoring log will provide evidence of the images which have been held and where they are kept. When deleted this should be recorded in the CCTV monitoring log.

Access to retained CCTV images is restricted to the Head and other persons as required and as authorised by the Head.

11. Complaints procedure

Complaints concerning the School's use of its CCTV system or the disclosure of CCTV images should be made in writing to the Head at Valley End School, Highams Lane, Chobham, GU24 8TB. Any complaint will be handled in accordance with the School's complaints policy.

All appeals against the decision of the Head should be made in writing to GST.

12. Monitoring Compliance

All staff involved in the operation of the School's CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.

All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to have undertaken the Educare Data Protection training.