CCTV policy

Dover College

Approved by:	James Ryeland	Date: May 2022
Last reviewed:	May 2022	
Next review due by:	April 2025	

Contents

1. Aims

This policy aims to set out the College's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on College property.

1.1 Statement of intent

The purpose of the CCTV system is to:

- Make members of the College community feel safe
- Protect members of the College community from harm to themselves or their property
- Deter criminality in the College.
- Protect College assets and buildings.
- Assist the police in deterring and detecting 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 defence of any litigation proceedings.
- Assist in the upholding of good order and discipline in the College.

The College will not use the CCTV system to:

- Encroach on an individual's right to privacy in spaces where they have a heightened expectation of privacy (including private residences, toilets and changing rooms)
- Pursue any other purposes than the ones stated above

The list of uses of CCTV are not exhaustive. Other purposes may be or become relevant.

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

Footage or any information gleaned through the CCTV system will never be used commercially.

In the unlikely event that the Police request that CCTV footage is 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 investigating a specific crime.

The footage generated by the system should be of good enough quality to be helpful to the police or the court to identify suspects.

2. Relevant legislation and guidance

This policy is based on:

2.1 Legislation

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

2.2 Guidance

- Surveillance Camera Code of Practice (2021)

3. 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*

4. Covert surveillance

Covert surveillance will only be used in extreme circumstances, such as suspicion of a criminal offence. If covert surveillance is needed, the proper authorisation forms from the Home Office will be completed and retained.

5. Location of the cameras

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

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

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

Cameras are not and will not be aimed off College grounds into public spaces or people's private property.

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

6. Roles and responsibilities

6.1 The Board of Governors

The Board of Governors are responsible for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with.

6.2 The Headmaster

The Headmaster 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 per 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.
- Review the CCTV policy to ensure the College complies with legislation.
- Ensure all persons authorisation to access the CCTV system and footage have received proper training from the DPO in using the system and data protection.
- Sign off on any expansion or upgrading to the CCTV system after taking advice from the DPO and considering the result of a data protection impact assessment.
- Decide whether to comply with disclosure of footage requests from third parties in consultation with the DPO.
- Carry out termly checks to determine whether the footage is being stored accurately and is deleted after the retention period.

6.3 The Data Protection Officer

The College IT Manager will be nominated as the Data Protection Officer (DPO) by default.

The Data Protection Officer will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system and 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 and assist the College with carrying out Data Protection Impact Assessments.
- Act as a point of contact for communications from the Information Commissioner's Office (ICO).
- Conduct Data Protection Impact Assessments.
- Ensure data is handled under 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.
- Keep accurate records of all data processing activities and make the records public on request.
- Inform subjects of how the College will use footage of them, their rights, and how the College will endeavour to protect their personal information.
- Ensure that the CCTV systems are working correctly and that the footage they produce is high quality so that individuals pictured in the footage can be identified.
- Ensure that the CCTV system is not infringing on any individual’s reasonable right to privacy in public spaces.
- Receive and consider requests for third-party access to CCTV footage.
- 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.
- Ensure the data and time stamps are accurate.

7. 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.

Recordings will be checked by the Headmaster termly and when the clocks change

8. Storage of CCTV footage

Footage will be retained for 30 days. The files will be overwritten automatically at the end of the retention period.

Occasionally, footage may be retained for longer than 30 days, for example, when a law enforcement body is investigating a crime, allowing them to view the images as part of an active investigation.

The College will download recordings to secure the data, and its integrity will be used as evidence if required.

The Headmaster will conduct termly checks to determine whether the footage is being stored accurately and deleted after the retention period.

9. Access to CCTV footage

The College will only give access to authorised persons to pursue the aims stated in Section 1.1 or if there is a lawful reason to access the footage.

Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log.

Any visual display monitors will be positioned so only authorised personnel can see the footage.

9.1 Staff access

The following members of staff have the authorisation to access the CCTV footage:

- The Headmaster (Mr Simon Fisher)
- The Bursar (Mr Andrew Hodkinson)
- The Data Protection Officer (Mr Wayne Bensted)
- The Assistant DPO (Mr Reece Waller)

- The Caretaker (Mr Richard Baxter)
- Anyone with the express permission of the Headmaster.

All members of staff who have access will undergo training to ensure proper handling of the system and footage.

Any member of staff who misuses the surveillance system may be committing a criminal offence and face disciplinary action.

9.2 Subject access requests (SAR)

According to UK GDPR and DPA 2018, individuals have the right to request a copy of their CCTV footage.

Upon receiving the request, the College will immediately issue a receipt and respond within 30 days during term time. Due to difficulties accessing appropriate staff members, the College reserves the right to extend that deadline during holidays.

All staff have received training to recognise SARs. When a SAR is received, staff should inform the DPO in writing. When making a request, individuals should provide the College with useful information such as the date, time, and location of the footage taken to aid College staff in locating the footage.

On occasion, the College will reserve the right to refuse a SAR if, for example, the release of the footage to the subject would prejudice an ongoing investigation.

Images that may identify other individuals must be obscured to prevent unwarranted identification. The College will attempt to conceal their identities by blurring out their faces or redacting parts of the footage. If this is not possible, the College will seek their consent before releasing the footage. If consent is not forthcoming, the still images may be released instead.

The College reserves the right to charge a reasonable fee to cover the administrative costs of complying with a repetitive, unfounded or excessive SAR.

Footage disclosed in a SAR will be disclosed securely to ensure only the intended recipient can access it.

Footage will be loaded onto a media storage device solely for that purpose and logged by the DPO.

Records will be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

Individuals wishing to make a SAR can find more information about their rights, making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

9.3 Third-party access.

The College will only share CCTV footage with a third party to further the aims of the CCTV system set out in section 1.1 (e.g. assisting the police in investigating a crime).

The College will only share the footage with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

All access requests should be written and sent to the Headmaster and the DPO.

The College will comply with any court orders that grant access to the CCTV footage. The College will provide the courts with the needed footage without unrestricted access. The Headmaster will carefully consider how much footage to disclose and seek legal advice if necessary.

The DPO will ensure that any disclosures are made in compliance with UK GDPR.

All disclosures will be recorded by the DPO.

10. Data Protection Impact Assessment (DPIA)

The College follows the principle of privacy by design. It is taken into account during every stage of the deployment of the CCTV system, including replacement, development and upgrading.

The system is used only to fulfil its aims (Section 1.1).

When the CCTV system is replaced, developed or upgraded, the College will carry out a DPIA to ensure the system's objective is still justifiable, necessary and proportionate.

The DPO will guide how to carry out the DPIA. The DPIA will be carried out by a Governor nominated by the Compliance and Risk Committee Chair.

Those whose privacy is most likely to be affected, including the College community and neighbouring residents, will be consulted during the DPIA. The College will put any appropriate safeguards in place.

The College will do a new DPIA annually or whenever cameras are moved or new cameras are installed.

If any unknown security risks are identified during the DPIA, the College will address them as soon as possible.

11. Security

- The DPO will be responsible for overseeing the security of the CCTV system.
- The DPO will check the system for faults before the start of each term.
- Any defects in the system will be reported as soon as they are detected and repaired as quickly as possible, according to the proper procedure.
- Footage will be stored securely and encrypted wherever possible.
- The CCTV footage will be password protected, and any camera operation equipment will be securely locked away when not used.
- The DPO will implement proper cyber security measures to protect the footage from cyber attacks.
- Any software updates (mainly security updates) published by the equipment manufacturer that needs to be applied will be employed as soon as possible.

12. Complaints

Complaints should be made according to the College's complaints policy which is displayed on the Dover College website or can be obtained in hard copy from the College Reception in Priory Lodge.

13. Monitoring

The policy will be reviewed every three years by a nominated Governor to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.

14. Links to other policies

- GDPR policy.
- Safeguarding policy.