ST. EDWARD'S OXFORD

CCTV POLICY

SEPTEMBER 2024

Document History

Document History	
Owner	Bursar
Document status	Approved
Approved by	Governing Body
This document is available from	School Intranet and School Website
Review Cycle	Annual
Current version adopted	August 2024
Next review date	August 2025
Linked documents	Data Retention Policy Data Protection Policy
Linked external documents	

1. Introduction

1.1 This policy sets out how St. Edward's School (the **School**) will manage the operation and use of CCTV.

1.2 The purposes of this policy are:

1.2.1 to help the School to regulate and manage its use of CCTV;

1.2.2 to help the School be transparent about how the School uses CCTV;

1.2.3 to help ensure that the use of CCTV remains a proportionate and justified response to the problems that it seeks to address; and

1.2.4 to provide guidance for all School staff on how to comply with data protection legislation in relation to the use of CCTV.

1.2.5 Enable pupils to contact supervising staff via Ring Doorbell systems.

1.3 This policy is aimed at members of staff working in the School (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, governors, contractors, agency staff, volunteers and any other visitor tothe School. It is available to pupils, parents, and visitors on request from the Sub Warden.

2. The Use of CCTV

2.1 The School's CCTV system comprises a number of cameras located on the School premises.

2.2 The School uses CCTV for the following purposes:

2.2.1 to safeguard the welfare of pupils, staff and visitors;

2.2.2 to protect the School, pupils, parents, staff and visitors from criminal activity such as theft and vandalism;

2.2.3 to increase personal safety;

2.2.4 to support the protection of property;

2.2.5 to aid in the investigation of accidents and incidents and the monitoring of health and safety; and

2.2.6 to support law enforcement agencies in the reduction, prevention, and detection of crime and to assist in the identification, apprehension and potentially prosecution of offenders.

2.3 CCTV footage may contain the personal information of those individuals captured by the recording.

3. Governance

3.1 The Estates Bursar has overall responsibility for the management and operation of the CCTV and the implementation of this policy.

3.2 The Estates Bursar will ensure that the CCTV system is operated according to this policyand that regular audits are carried out to ensure that the relevant procedures are compliedwith.

4. Minimising Privacy Risk

4.1 The School has carried out a Data Protection Impact Assessment on the use of CCTV. The outcome of the assessment was that the use of CCTV is a necessary and proportionate measure to achieve the purposes listed at 2.1 above provided that certain measures are put in place to mitigate the risks.

4.2 The School appreciates that the use of CCTV impacts on individuals' privacy but considers this intrusion to be justified because less privacy intrusive methods would not be sufficient to meet the School's purposes for using CCTV. In coming to this conclusion, the School has had particular regard to the safeguarding and welfare duties it owes to pupils.

4.3 The School reviews the Data Protection Impact Assessment on an annual basis to ensure that the use of CCTV continues to be justified and that the appropriate measures are in place to mitigate the data protection risks raised by its use.

4.4 The School will also review its use of CCTV should a concern be raised about its practices

5. The Operation of CCTV

5.1 The School has sited the cameras to view only areas which need to be monitored; for example, they do not monitor neighbouring private residences.

5.2 Where CCTV cameras are placed on the school premises the School displays signs to alert individuals that their image may be recorded. Such signs will identify the organisation operating the system, identify the purpose for using the surveillance system and whom to contact for further information, where these things are not obvious to those being monitored.

5.3 CCTV is not used in areas where individuals will have a heightened expectation of privacy; for example, there are no cameras in boarding houses or any toilets, changing rooms or bedrooms.

5.4 The cameras have been positioned in a way to ensure their security and to protect them from vandalism.

5.5 The School has ensured that the cameras can produce images of the necessary clarity and quality to meet the School's purposes.

5.6 Images can easily be extracted from the system if required, for example under a disclosure to

law enforcement agencies and or under a subject access request (please see section 11 for more information on subject access requests).

5.7 The CCTV does not capture sound recordings.

5.8 The CCTV cameras which record the perimeter of the School site are in operation 24 hours a day every day of the year because this is necessary to meet the purposes for whichthey were installed (for example, to detect intruders). The School is solely responsible for the operation of all CCTV in accordance with this policy for the purposes identified at section 2.1 above.

5.9 We will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or equivalent serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue. Any such monitoring or surveillance would be undertaken only on the decision of the Warden.

5.10 In the unlikely event that covert monitoring is considered to be justified, the School will carry out a Data Protection Impact Assessment (please see section 4 above for more information). The rights of individuals whose images may be captured will always be considered in reaching any such decision.

6. Maintenance of the CCTV Equipment

6.1 The IT Manager will check on a routine basis that the system is operating effectively and that the equipment is recording properly and that cameras are functional. Any software updates will be applied by the IT Manager.

6.2 The system will be regularly serviced and maintained to ensure that clear images are recorded. If any defects are found these will be reported to the IT Manager for rectification.

6.3 The School will monitor the operation of the CCTV system by investigating any notificationsor concerns regarding the functionality of the CCTV system.

7. Storage and Security

7.1 The CCTV footage will be stored securely and will only be accessed by designated Schoolstaff, being Estates Bursar, Security Manager, IT Manager, Warden, Sub-Warden, Safeguarding Leads and Bursar. Other staff may view the CCTV footage as and when required in exceptional circumstances with the permission of the Designated Staff. Designated Staff will be given additional training on CCTV, as appropriate.

7.2 CCTV recordings, including any copies made, are encrypted. The School will also encrypt any copy before it is shared with a third party (such as a law enforcement agency) unless there is a good reason for not doing so.

7.3 The Designated Staff are trained in the School's security procedures. The Designated Staff will ensure that camera footage is not accessed by any unauthorised person.

7.4 The only locations where CCTV footage can be viewed are in selected private and secure offices.

7.5 Only Designated Staff are authorised to make copies (electronic or paper) of the CCTV footage.

7.6 Only the Designated Staff may allow external persons or agencies to view the CCTV footage, and this will be done in accordance with section 12 below.

7.7 Any information security breach (for example, any unauthorised access to CCTV footage)must be reported immediately to the Compliance Manager in accordance with the School's Data Breach Policy.

7.8 All maintenance of ICT or CCTV equipment which could provide access to CCTV footage will only be carried out by the Designated Staff.

7.9 Staff should note that any misuse of the CCTV system might constitute a criminal offence,for example, accessing footage without authorisation from Designated Staff.

7.10 Where footage is saved following an incident this will be done securely.

8. Internal Use of the CCTV

8.1 If a member of staff considers that CCTV footage might be needed for an internal matter (e.g. a pupil disciplinary issue) they should speak to the Estates Bursar in the first instance.

9. Retention

9.1 Compliance with data protection law means that the School does not retain personal data for longer than is required for the purposes for which it was obtained. Recorded images will normally be retained for 30 days from the date of recording in accordance with the School's Data Retention Policy.

9.2 However, the School has procedures in place to retain information for a longer period if this is required. For example, where an incident caught by the CCTV footage is being investigated or where there has been a subject access request.

9.3 The School has procedures in place to ensure that information is disposed of securely. Thisis the responsibility of the IT Manager.

10. Informing Individuals about the use of CCTV

10.1 The School appreciates the importance of being open and transparent about the use of CCTV. This policy published on the School's website.

10.2 The School's privacy notices for staff, parents and pupils include information about the use of CCTV by the School including for what purpose it is used. A copy of the privacy noticescan be found on the school website.

10.3 There are prominently displayed signs in areas where CCTV is in operation (for example, at all access routes into and out of the School).

11. Subject Access Requests

11.1 Under data protection legislation individuals have the right to access information about themselves which may include images of them in CCTV footage.

11.2 Members of staff have been trained to recognise subject access requests and understand that such a request may cover CCTV footage. Staff must refer all subject access requests to the Compliance Manager immediately because such requests are complexand there is a statutory timeframe for the School's response.

11.3 Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the School's Subject Access Request Policy.

11.4 In order for us to locate relevant footage, any requests for copies of recorded CCTV images should include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

11.5 When such a request is made a member of the designated staff, the CCTV footage will be reviewed in accordance with the request.

11.5.1 If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The I.T Team as the CCTV system administrators must take appropriate measures to ensure that the footage is restricted in this way.

11.5.2 If the footage contains images of other individuals then the School must consider whether:

- The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals
- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained
- If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

11.6 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. The Data Protection Act 2018 provides data subjects (individuals to whom "personal data" relates) with a right to data held about them, including those obtained by CCTV.

11.7 A record must be kept (see Appendix A), and held securely, of all disclosures which sets out:

11.7.1 When the request was made

11.7.2 The process followed by the Head of IT (as the CCTV system administrator) in determining whether the images contained third parties

11.7.3 The considerations as to whether to allow access to those images

11.7.4 The individuals that were permitted to view the images and when

11.7.5 Whether a copy of the images was provided, and if so to whom, when and in what format.

11.8 Downloading Captured Data on to Other Media; In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures:

11.8.1 Each downloaded media must be identified by a unique mark.

11.8.2 Before use, each downloaded media must be cleaned of any previous recording.

11.8.3 The System Manager will register the date and time of downloaded media insertion, including its reference.

11.8.4 Downloaded 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 downloaded 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.

11.8.5 If downloaded media is archived the reference must be noted.

11.8.6 If downloaded media is put onto a device, the device will be encrypted and password

protected.:

12. Disclosure to Law Enforcement Agencies

12.1 Images from the CCTV system may be disclosed to law enforcement agencies (e.g. the Police) where the School considers such disclosure necessary (for example, for the prevention and detection of crime). However, any such disclosure will only be in accordance with data protection law.

12.2 Requests from law enforcement agencies should be referred to the Bursar.

12.3 If CCTV footage is disclosed to a law enforcement agency the School will record what information has been disclosed, when the disclosure was made, to whom the information was disclosed and for what purpose(s). The School has a register containing details of all disclosures of CCTV footage. The law enforcement agency should produce a written request using the appropriate form to support its request for disclosure. The School should keep a copy of this on file as well

12.4 The School will ensure that the disclosure of CCTV footage is carried out securely. The precise method of communication will be determined by the IT Director but encrypting the footage will be considered.

12.5 If law enforcement agencies require the School to retain the stored CCTV footage for possible use as evidence in the future the information will be indexed and securely stored until it is needed.

13. Other Requests for Information

13.1 Images from the CCTV system may be disclosed to law enforcement agencies (e.g. the Police) where the School considers such disclosure necessary (for example, for the prevention and detection of crime). However, any such disclosure will only be in accordance with data protection law.

13.2 Requests from law enforcement agencies should be referred to the Bursar.

13.3 If CCTV footage is disclosed to a law enforcement agency the School will record what information has been disclosed, when the disclosure was made, to whom the information was disclosed and for what purpose(s). The School has a register containing details of all disclosures of CCTV footage. The law enforcement agency should produce a written request using the appropriate form to support its request for disclosure. The School should keep a copy of this on file as well.

13.4 The School will ensure that the disclosure of CCTV footage is carried out securely. The precise method of communication will be determined by the IT Director but encrypting the footage will be considered.

13.5 If law enforcement agencies require the School to retain the stored CCTV footage for possible

use as evidence in the future the information will be indexed and securely stored until it is needed.

14. Contractors (also known as Processors)

14.1 If law enforcement agencies require the School to retain the stored CCTV footage for possible use as evidence in the future the information will be indexed and securely stored until it is needed

15. Breaches of this Policy

15.1 If staff consider that this policy is not being followed in any respect, they must inform the Compliance manager immediately.

15.2 Any breach of this policy by a member of staff will be taken seriously and may result in disciplinary action.

16. Legal Basis of Processing

16.1 Under data protection law the School must set out the bases it is relying on to make anduse CCTV footage.

16.2 The School considers that the following bases are applicable:

16.2.1 The School has a legitimate interest in using CCTV for the purposes described at paragraph 2.2 above. In addition, others, such as pupils, parents, and visitors to the School site, also have a legitimate interest in the School's use of CCTV (e.g. so that they are confident that the School site is safe). The use of CCTV is not unfair because the School has put measures in place to safeguard the rights of individuals identifiable from CCTV, as described in this policy. The School considers that the use of CCTV is necessary for the purposes described at paragraph 2.2.

16.2.2 The use of CCTV for the purposes described in paragraph 2.2 is also in the public interest.

16.2.3 Sometimes the School's use of CCTV will be necessary for compliance with a legal obligation, for example, where it is required to disclose a CCTV recording to the Police in accordance with a court order.

16.3 There may be other bases depending on the circumstances

17. Complaints

17.1 Any complaints or concerns about the use of CCTV by the School should be addressed to the

Bursar.

18. Ring Doorbell and Camera Systems

18.1 Ring Doorbell Systems enable pupils to contact supervising staff from secured areas at night from within the boarding house.

18.2 This system can view the cameras live and view saved events. It also has the ability for two-way conversation.

18.3 The system operates over the schools Wi-Fi system.

18.4 The School has one subscribed account holder, the Estates Bursar, who shares access to devices with selected staff so it can be viewed on their Ring Account App.

18.5 Authorised users and Designated Staff can have two-way conversation, if enabled, anywhere the internet is available either over Wi-fi or 4/5G.

18.6 The Estates Bursar can add or remove staff users at any time.

18.7 The Estates Bursar will provide the IT department with the account log in credentials forback up and to enable access by any member of the SMT with the Sub-Warden's written authorisation.

18.8 Ring Doorbells in boarding houses have the video element disabled.

18.9 Ring Doorbells on entrance doors to offices, teaching facilities and private residences have the record event function enabled with live view and two-way voice.

18.10 Ring Camera units may be installed in locations where the supervision of pupils is not always visually possible, such as boarding house gardens. Notices will be prominently displayed, as for CCTV cameras.

18.11 Ring Camera units may have the record history enabled for the purposes of external security and pupil behaviour monitoring in external locations only (outside).

18.12 The use of recordings for the purposes of a disciplinary process as evidence is not permitted without the written consent of the Warden or Sub-Warden.

18.13 The downloading of event footage is not permitted without the written consent of the Warden or Sub-Warden.

18.14 Recordings may be provided to the Police upon request.

18.15 The position of any Ring Doorbell or Camera unit is to be approved by the Designated Safeguarding Lead

18.16 The maintenance and upkeep of all Ring Systems are the responsibility of the Estates department.

18.17 Event recordings are kept on the Ring Server for 30 days unless deleted by the Estates Bursar sooner. Recordings will only be actively deleted with the written authorisation of the Sub-Warden.

18.18 Live and recorded view is to be kept disabled inside when fitted inside boarding houses – so voice only.

Appendix A – Record Keeping of CCTV Images

- Access to view and record footage, as well as to the folder where data is saved, is limited to the designated staff per this policy.

- Details relating to any footage downloaded for investigative purposes must be recorded in the CCTV download register maintained by the Estates Bursar. The details to be maintained include:

    - Date footage downloaded
    - User storing the footage
    - File name
    - Incident date
    - Brief incident description
    - Reason for retention
    - Featured parties

- The downloaded footage is saved in the relevant folder for the academic year with the tile being specific to camera name and individual's initials in the images recorded.

All employees who have access to this area of the network are aware of the restrictions in relation to access to, and disclosure of, recorded images.