CCTV Policy

Date ratified	May 2023
Committee Responsible for Policy	Business Committee and FGB
Date to be updated	May 2026
Headteacher Signature	
Chair of Governors/ Committee Signature	

Holy Trinity has adopted the Merton model CCTV Policy June 2019

1. Purpose and Legislative Context

1. This School is committed to the safety of its students, employees and visitors. The use of CCTV in line with this Policy forms part of this commitment. Specifically, this Policy aims to:
    a. Ensure that CCTV recordings are only accessed or used when appropriate, in line with procedural and legal requirements;
    b. Assist the management of our school;
    c. Protect our premises and assets from physical damage;
    d. Increase personal safety and reduce instances of aggression or crime;
    e. Support investigations of known or suspected instances of inappropriate behaviour, aggression or physical damage. This may include investigations by the police when criminal activity is suspected;
    f. Assist with the identification, apprehension and prosecution of offenders.

2. This Policy has been drafted with due regard to the requirements of legislation and statutory guidance, including but not limited to:
    a. The Data Protection Act 2018;
    b. The Regulation of Investigatory Powers Act 2000;
    c. Information Commissioner's Office Code of Conduct for CCTV;
    d. The Freedom of Information Act 2000 and the Freedom of Information and Data Protection Regulations 2004;
    e. The Equality Act 2010;
    f. The Protection of Freedoms Act 2012;
    g. The Children Act 1989 and the Children Act 2004;
    h. The Education (Pupil Information) (England) Regulations 2005, as amended;
    i. Article 8 of the Human Rights Act 1998.

3. This Policy operates alongside the following policies, which are available on our website:
    a. Behaviour
    b. Data Protection;
    c. Safeguarding and Child Protection.

4. The CCTV System will be managed in line with the following data protection principles.
    a. Processed lawfully, fairly and transparently.
    b. Collected for legitimate purposes only, as specified by this Policy and guided by relevant legislation or guidance;
    c. Limited to what is necessary and proportionate to the legitimate purposes;
    d. Accurate, up to date and destroyed if it is not accurate or up to date;
    e. Stored in line with our Data Protection Policy, Data Retention Schedule and data protection legislation or guidance;
    f. Processed securely and not lost, destroyed, damaged or processed in an unauthorised way.
5. Monitoring and review: This Policy will be reviewed at least every three years. Advice will be sought from our DPO as appropriate.

6. Employee Conduct: Employees are strongly advised to consider the importance of the right to privacy, of the integrity of personal data, and of the right not to be discriminated against because of a protected characteristic. If employees use or access CCTV equipment or footage in a way that goes against these rights or values, they will be sanctioned in line with our Disciplinary procedures. External agencies will be informed as appropriate, including the police where required.

2. Location of CCTV Cameras

7. The CCTV system operates 24 hours a day, every day of the year.

8. Where CCTV cameras are located: We use CCTV cameras to monitor activity in key areas of our premises, including entranceways, car parks and other external public areas. This is to:
    a. Identify known or suspected instances of aggression or crime;
    b. Secure the safety and well-being of students, employees and visitors.

9. Where CCTV cameras are not located:
    a. We do not use CCTV cameras in class rooms, offices, meeting rooms or in areas where there is an increased expectation of privacy.
    b. We do not use CCTV cameras to record activity on private property (e.g. homes and gardens in the surrounding community).

10. Signage/Notices: Prominent notices, as required by the ICO Code of Practice for CCTV use, are located at all access routes to areas monitored by CCTV cameras.

11. Forbidden use of CCTV cameras:
    a. CCTV cameras must not be used to conduct covert surveillance (whereby subjects are not informed) and we do not have the authorisation to conduct covert surveillance.
    b. Unless an immediate response to an incident is required, CCTV cameras must not be directed or targeted at individuals, their property or a specific group of individuals, unless authorisation is obtained using the Home Office Application Form for Directed Surveillance. If granted, authorisation will last for up to 3 months.
    c. CCTV cameras must not be used for any purpose other than those set out in this Policy and in relevant legislation or statutory guidance. d. Access to CCTV footage must be in line with Section IV of this Policy.

12. CCTV Control. Monitors are installed in the School Office and Site Manager's Office, to which pictures are continuously recorded.

3. Management

13. For the purposes of this Policy, this school is the data controller (i.e. an individual or organisation that determines the purposes and the means of processing personal data). The data controller is responsible for ensuring that CCTV footage is recorded and processed legally, fairly, proportionately and for legitimate purposes.

a. The Headteacher and governing body have overall responsibility for overseeing the use of the CCTV System in line with this Policy and relevant legislation or guidance.

14. The Data Protection Officer is responsible for implementing the Data Protection Policy and coordinating freedom of information requests or subject access requests in line with that Policy and with data protection legislation or guidance. In relation to the CCTV System, the Data Controller is responsible for working with the Data Protection Officer to ensure that:
    a. The CCTV System is registered with the ICO;
    b. The installation of any additional CCTV equipment is subject to a Data Protection Impact Assessment (DPIA);
    c. Identifying data protection or security risks of existing or proposed CCTV equipment and working to address those risks with relevant colleagues and external agencies, as appropriate;
    d. We handle and process CCTV footage in line with the Data Protection Policy and data protection legislation;
    e. CCTV footage is obtained, stored and in line with our Data Protection Policy and data protection legislation;
    f. CCTV footage is destroyed securely in line with our Data Protection Policy, our Retention Schedule and data protection legislation;
    g. Informing data subjects of how their personal data will be captured by the CCTV system, of their rights in relation to the access to and destruction of CCTV footage which contains their personal data, and of the measures implemented to protect data subjects' rights.

15. Day-to-day management of the system is the responsibility of the Premises Manager.

4. Access to CCTV Equipment and CCTV Footage

16. All equipment or devices containing CCTV footage or images belong to the school as the data controller.

17. The "CCTV Request to View Form" (Appendix A) should be used to submit and authorise requests to access data obtained by the CCTV System.

18. CCTV control equipment is only accessible to members of SLT, Headteacher and Premises Manager.

19. When viewing footage:
    a. It is only necessary to show CCTV footage to other employees if the individual(s) recorded in the footage cannot be identified by members of SLT, Headteacher and Facilities/Operations Manager, and if the employees with whom the footage is shared are likely to be able to identify those individuals;
    b. Visitors must be accompanied by members of SLT, Headteacher and Facilities/Operations Manager;
    c. If maintenance is required, the members of SLT, Headteacher and Facilities/Operations Manager must be satisfied of the identity and purpose of contractors before allowing entry;
    d. A log book is stored securely to record the identity of visitors and the time and date of their entry and exit;
    e. Equipment must be locked away at all times unless the members of SLT, Headteacher and Facilities/Operations Manager is present;

f. Emergency procedures may be used in exceptional cases when the support of the emergency services is required.

20. Third Party Access:
    a. Third party requests to access data captured by the CCTV System should be assessed by the DPO and the relevant school staff or a suitable representative from the SLT.
    b. Recordings may be viewed by the police for the prevention and detection of crime (DPA 2018).
    c. Viewing of recordings by the police will be recorded in writing and in the log book
    d. Footage required for evidential purposes by the police must be copied onto a separate USB drive or disc, sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence store.
    e. Recordings will only be released to the police on the clear understanding that the recording remains the property of the school; and that both the recording and information contained on it are to be treated in accordance with our Data Protection Policy and relevant legislation or statutory guidance;
    f. If a court requires the release of an original recording, this will be produced from the secure evidence store in a sealed bag;
    g. The police may ask us to retain footage for possible use as evidence in the future. Such footage will be properly indexed and securely stored until needed by the police and in line with the Data Protection Policy and relevant legislation or statutory guidance,
    h. Applications received from other third parties (e.g. solicitors), to view or release recordings, will be referred to the Headteacher, DPO and legal advisers where required.

21. Access by Data Subjects.
    a. Data subjects have a right to obtain confirmation that their personal data is being processed.
    b. Data subjects have the right to submit a subject access request to gain access to their personal data, including data obtained by CCTV.
    c. Subject access requests will be referred to the Headteacher and managed in line with the Data Protection Policy and relevant legislation or statutory guidance.
    d. We reserve the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

5. Storage, Retention and Destruction

22. Data obtained by the CCTV System is stored and retained and securely destroyed in line with our Data Protection Policy, Retention Schedule and relevant legislation or statutory guidance

23. CCTV footage is stored on controller hard drives for 30 days.

24. CCTV footage must never be stored on personal USB drive and photos must never be taken of CCTV footage on personal mobile devices.

25. Password protected USBs are securely stored.

26. CCTV footage must only be transferred to the USBs by, designated staff, when it is necessary to store footage for longer than the time it is stored on the hard drives (e.g. because an investigation is on-

going or because there is reasonable cause to believe that the footage will be needed for a future investigation);

27. CCTV files stored on the USBs must be named by date and time.

28. The transfer of CCTV footage to USB and the reason(s) for the transfer must be recorded in the log book and signed off an appropriate member of staff.

29. CCTV files stored on USBs must only be accessed by appropriate members of staff.

30. If footage is archived in line with our Data Protection Policy and data protection legislation or guidance, then it must be given a unique reference number (i.e. the camera location; and the date and time of the recording), logged and stored securely

APPENDIX A: CCTV REQUEST TO VIEW FORM

Date	
Name of Person Requesting Access	
Contact Details	
Authoriser's name	
Reason for request (e.g. known or suspected criminal activity).	
Include date and time of the incident (an approximate time window is acceptable).	
Declaration by the authoriser I authorise access to the requested CCTV data by the above named person(s); and that I have clearance to authorise such access.	
Signed	
Declaration by the person requesting access – I understand that: The data accessed must be used in accordance with the CCTV Policy, the Data Protection Policy and data protection legislation or guidance; and that data remains the property of the school, which may refuse permission for the data to be passed onto any other individual or organisation.	
Signed:	

APPENDIX B: CCTV SIGNAGE

It is a requirement of the Data Protection Act 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 purposes of using CCTV
- The name of the School.
- The contact telephone number or address for enquiries.

Example Sign

WARNING
CCTV cameras in operation
Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behaviour, the prevention of bullying, for the safety of our staff and students 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 School
For more information contact .....*<phone number>*.....