Holy Trinity C of E Primary Academy

Vision Statement
At Holy Trinity CE Primary Academy, inspired by and rooted in Christian values and teaching, we nurture children to become aspirational, courageous, compassionate and joyful young people.

The values of our school: Courage, Joy, Aspiration and Compassion

POLICY DOCUMENT	**School CCTV policy**
Status	Statutory
Legislation	General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA)
Lead Member of Staff	Headteacher
Lead Governor (Monitoring)	Jeremy Shatford
Governor Committee	FGB
Approval Date and by	November 2022
Review Frequency	Annual
Date of next review	Next review November 2022

1 Introduction

1.1 The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the School and ensure that:

- We comply with the UK-GDPR, and Data Protection Act 2018.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation and their rights are being upheld.

1.2 CCTV – Closed Circuit Television is a system of cameras which stream an image to a central monitor, where activity can be recorded.

1.3 This policy covers the use of our CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing
- Taking action to prevent a crime

2 About this policy

2.1 This policy has been created regarding the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office (ICO) (2014) 'CCTV Code of Practice'

2.2 This policy has due regard to legislation including, but not limited to, the following:

- The General Data Protection Regulation 2016
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Protection of Freedoms Act 2012
- The Regulation of Investigatory Powers Act 2000
- The UK-GDPR 2021

2.3 This policy operates in connection with the following School policies:

- Data Protection and Freedom of Information Policy.
- Photographs & Video Policy.

3 The Data Protection Principles and Privacy by Design

3.1 Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- 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 for no longer than is necessary for the purposes for which the personal data are processed.
- 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.

3.2 The Academy has followed the ICO's guidelines on Privacy by Design – before planning installing and using a surveillance system, the School has:

- Considered whether the School can fulfil its requirements through a less privacy-intrusive system that does not include surveillance and recording.
- Carry out a Data Privacy Impact Assessment (DPIA) to assess security risks and how the rights of individuals will be upheld.

4 Responsibilities of the School

4.1 The School as the corporate body, is the data controller. The governing board of XXX therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

4.2 The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate, and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration, and disclosure.

5 Responsibilities of the Data Protection Officer

5.1 As a School we are data controllers in law and are required to appoint a Data Protection Officer. Our DPO is Jeremy Shatford and can be contacted at mailto:dpo@jeremyshatford.co.uk?subject= CCTV

5.2 The DPO is responsible for ensuring compliance with the Data Protection legislation and with this policy. Their responsibilities are laid out in the Data Protection policy, but in relation to CCTV and surveillance they include:

- Ensuring that all data controllers at the School handle and process surveillance and CCTV footage in accordance with the 6 data protection principles.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Supporting the School to complete a Data Privacy Impact Assessment when installing or replacing cameras.
- Reviewing the effectiveness of the current CCTV system and making recommendations if appropriate.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the School, their rights for the data to be destroyed and the measures implemented by the School to protect individuals' personal information.

6 Responsibilities of the Governing Body

6.1 The governing body has the following responsibilities:

- Meeting with the DPO to decide where CCTV or BWC is needed to justify its means.

- Liaising with the DPO regarding the lawful processing of the surveillance and CCTV footage.
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the School is using surveillance fairly and lawfully.
- Communicating any changes to legislation to all members of staff.

7 Purpose and justification

7.1 Surveillance will be used as a deterrent for theft and vandalism to the School.

7.2 The School may share surveillance footage to assist the police in identifying persons who have committed an offence.

7.3 The School will only conduct surveillance as a deterrent and will not site cameras in classrooms or any changing facility.

7.4 In the unlikely event that a child or member of staff from the academy is identified via CCTV images causing damage to the school, those images may be used as part of disciplinary and grievance processes. This will be communicated to pupils and staff through the School Privacy Notices.

7.5 In limited circumstances, Holy Trinity CE Primary Academy might also use evidence of arrival/departure times of contracted services to prevent financial loss to the academy.

7.6 If the surveillance and CCTV systems fulfil their purpose and are no longer required, it will be deactivated.

8 How Holy Trinity CE Primary Academy manages CCTV and surveillance

8.1 The School is registered as a data controller with the Information Commissioner's Office, which also covers the use of surveillance systems.

8.2 In areas where CCTV is used, the School will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area. The signs contain details of the purpose for using CCTV e.g., public safety or crime prevention along with how to get further information.

8.3 The surveillance system is a closed digital system will not record audio by default., as audio recording may be considered an excessive intrusion of privacy.

8.4 The CCTV system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered, and 'blind' spots may exist.

8.5 The CCTV cameras are installed to show the following locations within the school grounds...

- The vehicular gate and some of the field
- The Pedestrian gate and some of the playground
- The staff car park and the gates leading out from the car park

8.6 The CCTV system is static, and cameras are not trained on property outside the perimeter of the school. The system may pick up private vehicles which enter the school's grounds via the staff car park.

8.7 The school uses a closed digital system which does not record audio. The video footage is held on the school network and can only be accessed by authorised personnel.

8.8 The authorised persons will be controlled and granted by the Data controller. The school's authorised CCTV system operators are:

- The Headteacher – Anna Woodman
- The Assistant Headteachers – Dorian Amor and Mark Gyllenspetz
- The business Manager Caron Yates

- Admin Officer Ruth Edwards

8.9 The system is only active outside normal school hours on the following schedule

- 4pm – 8am weekdays
- 24-hour coverage during weekends & school holidays

8.10 Data will normally be retained for 2 weeks and then destroyed. The CCTV system will be tested for security flaws annually to ensure that they it is being properly always maintained. This annual service will be undertaken by the schools authorised contractor. Any cameras that present faults will be repaired as soon as reasonably practicable as to avoid any risk of a data breach.

8.11 The surveillance system has been designed for maximum effectiveness and efficiency; however, the School cannot guarantee that every incident will be detected or covered and 'blind spots' could exist.

8.12 The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

8.13 The surveillance system will not be trained on private vehicles or property outside the perimeter of the School.

9 Security

9.1 Access to the surveillance system, software and data is strictly limited to authorised school staff and is password protected.

9.2 The school 's authorised CCTV system users are:

- The headteacher.
- The School Business Manager and Administration Officer.
- Authorised maintenance technicians.

9.3 Visual display is via computer monitors are in the administration office and are password protected and always locked when not in use. The screen is not in sight of the public and is turned off when there is no requirement to view live images.

9.4 Surveillance and CCTV systems will be tested for security flaws once a term to ensure that they are being properly always maintained.

9.5 Any unnecessary footage captured will be securely deleted/overwritten from the system.

9.6 Any cameras that present faults will be repaired immediately to avoid any risk of a data breach.

10 Storage and retention of images

10.1 Recorded data will not be retained for longer than is necessary. 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.

10.2 The CCTV images will be automatically overwritten on a fortnightly cycle, though this may be longer in school holidays. Data will not be retained beyond the point it is automatically overwritten by new recordings unless it has been extracted in the process of reporting crimes to the police or where the footage needs to be stored for longer periods as part of a legal matter.

10.3 All retained data will be stored securely and will be listed on the school 's Data Asset Audit.

10.4 All retained data must be stored in a searchable system. Only a primary copy should be kept, and secondary copies should only be created in exceptional circumstances.

11 Subject Access Requests (SARs)

11.1 Individuals have the right to request access to video footage relating to themselves under the Data Protection Act 2018.

11.2 The DPO must be informed and consulted for any such requests.

11.3 All requests should be made to the Headteacher or the Data Protection Officer. 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. Requests may be written or verbal.

11.4 The school will immediately indicate receipt and will determine it any CCTV footage still exists, if so, will then respond within one calendar month of receiving the request.

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

11.6 All attempts will be made to allow the viewing of the video. If others can be identified, the School will assess the risk to others from the video being viewed by the requester. If there is likely to be a risk of harm, the school may consider the following options where appropriate:

- Obtain the consent of others to share the video with the requester.
- Use video-editing software to blur the faces of others who can be identified from the video.
- Provide selected still images from the video and blur the identifiable faces.
- Provide a transcript or written description of the contents of the video.

11.7 If all options have been considered and the school still consider there to be a risk to others from the requester viewing the video, the school may decline the request to view the video (although relevant exemptions in the Data Protection Act 2018 will need to be identified by the school provided to the requester).

11.8 The school will not provide copies of the video to others unless instructed to do so in law or there is no risk to individuals who may be identifiable from the video.

12 Access to and disclosure to other third parties

12.1 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) and with the correct authorisation.

12.2 Requests from third parties should be made in writing to the Headteacher/Governing Body or the Data Protection Officer.

12.3 Consideration will always be given to the safeguarding and best interest of pupils. Data Protection will not be used as an excuse to prevent the viewing of images if there is an overwhelming need. All disclosures and the reasons for release should be recorded.

12.4 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. This will be communicated to staff through the School Privacy Notices.

13 Complaints

13.1 Complaints and enquiries about the operation of CCTV within the School should be directed to the Headteacher/Governing Body or the Data Protection Officer in the first instance.

14 Review

14.1 This policy will be reviewed every year.

November 2021	New insert 7.5 extending the purpose. 8.8 name change
Date of next review	**November 2022**

18 Appendix One: CCTV Data Retrieval Log

Anyone accessing the CCTV will need to complete this log

Name	Date Accessed	Time accessed	Reason (inc time and date of subject matter)