



CCTV Policy

Audience: Staff, visitors, contractors, parents/carers (for transparency)

Owner: Judicium (Data Protection Officer, dataservices@judicium.com) with Ian Love, School Business Manager, as CCTV System Manager

Statutory basis: UK GDPR; Data Protection Act 2018; Protection of Freedoms Act 2012; ICO CCTV Code of Practice

Approval: Governing Body

Review cycle: Every 2 years (or sooner if systems/processes change)

Last reviewed: October 2025

Next review due: October 2027

1. Purpose and objectives

Dorchester Primary School uses CCTV to support safeguarding, safety and security on the school site. Objectives are to: (i) protect pupils, staff and visitors from harm; (ii) protect buildings and assets; (iii) deter, prevent and detect crime; (iv) assist the police with investigations; (v) identify, apprehend and prosecute offenders; (vi) establish the cause of accidents/incidents and prevent re-occurrence; and (vii) assist with site management.

2. Scope and system description

This policy regulates the management, operation and use of the school's CCTV system. The system consists of fixed cameras positioned where they are most effective for the purposes above. CCTV is not installed in areas where individuals reasonably expect privacy (e.g. toilets). The school does not record audio. If any future deployment requires audio or placement in a privacy-sensitive area, the school will complete a Data Protection Impact Assessment (DPIA), consult stakeholders as appropriate and provide prominent additional signage before activation.

Camera inventory:

Camera ID	Location	Type (fixed/PTZ)	Audio (Y/N)	Recording Capacity	FoV/Notes
1.	Front L/H corner.	Fixed Bullet	N	Approx 1 Month	
2.	Main Entrance.	PTZ	N	Approx 1 Month	
3.	Main Entrance.	Fixed Bullet	N	Approx 1 Month	
4.	Reception Office.	Fixed Dome	N	Approx 1 Month	
5.	Hall Section 1.	Fixed Dome	N	Approx 1 Month	
6.	Hall Section 2.	Fixed Dome	N	Approx 1 Month	
7.	Outside Hall covering L/H area.	Fixed Bullet	N	Approx 1 Month	
8.	Outside Hall covering R/H area.	Fixed Bullet	N	Approx 1 Month	
9.	Rear Playground	PTZ	N	Approx 1 Month	
10.	Rear Playground Walkway RHS	Fixed Bullet	N	Approx 1 Month	
11.	Rear Playground Walkway LHS	Fixed Bullet	N	Approx 1 Month	
12.	Nursery Perimeter.	Fixed Dome	N	Approx 1 Month	
13.	Nursery Gate	Fixed	N	Approx 1 Month	
14.	Middle Gate (outside Hall)	Fixed	N	Approx 1 Month	
15.	Bike Store	Fixed	N	Approx 1 Month	
16.	Main Entrance Walkway / Gate	Fixed	N	Approx 1 Month	
17.	Car Park & Gate	Fixed	N	Approx 1 Month	Wireless transmission

3. Lawful basis, DPIA and signage

Processing is necessary for the school's legitimate interests (Article 6(1)(f) UK GDPR) and for the performance of tasks in the public interest (Article 6(1)(e)), namely safeguarding and site security. The school maintains a DPIA for CCTV and updates it whenever significant changes are proposed. Clear signs are displayed at site entrances and within the site stating that CCTV is in operation.

4. Statement of intent

Cameras are installed visibly; the school does not use covert recording. The system is designed to avoid intruding on neighbouring private property so far as possible. Images are not used for commercial purposes. Images will be disclosed to the media only with police written authority for investigation of a specific crime and never for entertainment.

5. System management and access controls

The CCTV System Manager is the School Business Manager. In their absence, the Headteacher will act. Access to live view/recordings is password-protected and restricted to the System Manager, their deputy and senior leaders authorised by the Headteacher. The system is intended to operate 24 hours a day, 365 days a year; availability cannot be guaranteed. The System Manager checks functionality and recording regularly and records checks in the CCTV log. Unless an urgent response is required, cameras will not be directed at an individual or a specific property without authorisation under the Regulation of Investigatory Powers Act 2000 (RIPA). Where used wireless camera transmissions are encrypted to prevent interception.

6. Storage, retention and security

Images are retained only for as long as necessary for the purposes stated. The system overwrites recordings automatically after approximately 30 days. Where footage is required for an ongoing investigation, disciplinary, insurance claim or legal proceedings, relevant clips are securely retained for as long as necessary and then deleted. Servers/recorders are kept in a secure area with restricted access.

7. Downloading, disclosure and evidential handling

To maintain integrity and admissibility, any footage exported to portable media will be uniquely referenced, created from a clean medium, logged (date/time/reference), sealed and stored in a secure evidence store. If the police request footage, a copy will be supplied on the understanding that it remains the property of the school and must be handled in accordance with data protection law. The school keeps a record of all viewings and disclosures. Where practicable, potential witnesses will avoid viewing footage prior to police request.

8. Requests from individuals and third parties

Individuals have the right to request access to personal data (images in which they are identifiable). Requests should be made to the school's Data Protection Officer (DPO) at dataservices@judicium.com. Requests from third parties (e.g. parents/solicitors) will be considered by a senior leader in consultation with the DPO; only footage that can be disclosed lawfully (e.g. with third-party redaction or a suitable lawful basis) will be released.

9. Complaints

Complaints about the operation of the CCTV system should be addressed to the Headteacher in the first instance, following the school's Complaints Procedure.

10. Roles and responsibilities

The Governing Body approves this policy and monitors compliance. The Headteacher ensures implementation. The DPO advises on data protection compliance, DPIA and data subject rights. The System Manager operates the system day-to-day, maintains the asset/register and logbook, manages user access and ensures checks and maintenance are completed.

11. Monitoring, review and training

This policy and the CCTV DPIA are reviewed at least every two years and whenever there is a significant change to the system. Staff with access to CCTV receive appropriate training and are made aware of their responsibilities.

12. Related documents

- Data Protection Policy and Privacy Notices
- Behaviour and Anti-Bullying Policy
- Safeguarding & Child Protection Policy
- Health & Safety Policy
- Complaints Procedure
- Records Management & Data Retention Schedule
- DPIA: CCTV

Version Control

Version	Date	Author	Changes	Approved by
1.0	October 2025	Data Protection Officer / Headteacher	New policy aligned to Judicium model; Dorchester house style	Governing Body