

CCTV Policy	
Policy area	GDPR
Policy Author	Headteacher
Status	Draft / Approved
Category	School Specific
Implementation Date	Autumn Term 26
Review cycle	3 Years
Next review date	Autumn Term 29

Document Control

Date	Version	Comments
Summer 2026	V2	SJo adjusted

Contents

1	Declaration of Intent	2
2	Legal Framework	2
3	Definitions	2
4	Roles and Responsibilities.....	2
5	Purpose and Justification.....	3
6	Data Protection Principles.....	3
6.1	Lawful Basis (UK GDPR Article 6)	3
6.2	Records of Processing Activities (UK GDPR Article 30).....	4
7	Objectives	4
8	Protocols	4
9	Security	4
10	Retention and evidence handling.....	5
11	Privacy by Design (DPIA)	5
12	Code of Practice	5
13	Access (Subject Access Requests & Disclosure)	6
14	Monitoring and Review	7
15	Equality, Safeguarding and Data Protection Statement	7
16	Contact.....	7
17	Appendix A (informative): Typical camera locations (high-level).....	7

1 Declaration of Intent

Clapham and Patching uses CCTV to help maintain a safe environment for pupils, staff, visitors and contractors; deter and detect crime; and protect school property. This policy sets out how the school manages and regulates CCTV in line with UK GDPR and the ICO's surveillance guidance.

2 Legal Framework

This policy has due regard to, including but not limited to:

- Regulation of Investigatory Powers Act 2000 (RIPA)
- Protection of Freedoms Act 2012
- UK General Data Protection Regulation (UK GDPR)
- Freedom of Information Act 2000 and related Fees Regulations
- Education (Pupil Information) (England) Regulations 2005 (as amended 2016)
- School Standards and Framework Act 1998; Children Act 1989; Children Act, 2004; Equality Act 2010

It is informed by: Home Office *Surveillance Camera Code of Practice* (2021) and ICO guidance on CCTV and GDPR.

3 Definitions

- Surveillance: Monitoring movements/behaviour of individuals; for this policy, video (and any associated audio where applicable).
- Overt surveillance: CCTV openly deployed with signage.
- Covert surveillance: Intentionally hidden surveillance; only in exceptional circumstances and in accordance with RIPA.

4 Roles and Responsibilities

- **Data Controller:** Clapham and Patching (governing body) has overall responsibility for ensuring CCTV processing complies with data protection legislation. Day-to-day data controller function is delegated to the Chief Finance & Operating Officer (CFOO). The Data Controllers role will include oversight of and ensuring that:
 - surveillance and CCTV footage is processed legally and fairly.
 - surveillance and CCTV footage is collected for legitimate reasons and ensuring that it is used accordingly.
 - surveillance and CCTV footage that is collected is relevant, adequate and not excessive in relation to the reason for its collection.
 - any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
 - footage containing personal data is protected against accidental, unlawful destruction, alteration and disclosure, especially when processing over networks.
 - comprehensive and accurate records are kept of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.

- data subjects are informed 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.
- The role of the **headteacher** includes:
 - Making decisions where CCTV is needed to justify its means.
 - Seeking appropriate guidance with regard to 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 with all members of staff.
- **Data Protection Officer (DPO):** SchoolPro (advises on lawful processing and DPIAs; reports to the highest level of governance).
- **Headteacher:** Justifies CCTV use, ensures policy compliance, leads investigations into any breaches, and authorises viewing/disclosure.
- **Office Manager:** Day-to-day operational lead for the CCTV system (system checks, ensuring cameras function and record correctly).
- **Network Manager:** Administers IP cameras in specified locations (e.g., Inclusion and Behaviour offices) and manages the IT DVR.

5 Purpose and Justification

Clapham and Patching deploys CCTV solely to: deter criminal acts and antisocial behaviour; protect assets; promote the health, safety and welfare of pupils, staff and visitors; and assist law enforcement. CCTV is not installed in changing facilities and is not trained on private homes or gardens outside the site perimeter. If CCTV ceases to meet these purposes it will be deactivated or re-scoped.

6 Data Protection Principles

All CCTV processing at the school will be:

- Lawful, fair, transparent;
- Limited to specified, explicit, legitimate purposes;
- Adequate, relevant, and limited to what is necessary;
- Accurate and kept up to date where necessary;
- Kept no longer than necessary;
- Secured appropriately (integrity and confidentiality).

6.1 Lawful Basis (UK GDPR Article 6)

The school relies on **legitimate interests (Article 6(1)(f))** as the lawful basis for processing personal data via CCTV. The legitimate interests pursued are the safety and security of pupils, staff, visitors and contractors, the protection of school property, and the prevention and detection of crime. A Legitimate Interests Assessment (LIA) has been completed and is held on file. The school is satisfied that these interests are not overridden by the rights and freedoms of the

individuals whose data are captured, having regard to the safeguards set out in this policy and the supporting DPIA.

6.2 Records of Processing Activities (UK GDPR Article 30)

CCTV processing is recorded in the school's Record of Processing Activities (ROPA), which is maintained by the DPO and reviewed at least annually. The ROPA entry documents the purposes of processing, categories of data subjects, retention periods, and security measures.

7 Objectives

The CCTV system is used to: maintain a safe environment; ensure welfare; deter criminal acts; assist police in identifying offenders; and support the effective management of the school.

8 Protocols

- **System type:** Closed digital system.
- **Registration:** The system is registered with the ICO as required by data protection legislation.
- **Signage:** Clear notices are displayed at all access routes to areas covered by CCTV.
- **Coverage:** Cameras are positioned for maximum effectiveness; 'blind spots' may exist; cameras will not be trained on private property or individuals unless an immediate response to an incident is required.

Clapham and Patching -specific camera deployment

- Fixed cameras are sited at the entrance to the school carpark and driveway and the front of the school building reception area.
- IP cameras are located in the Office Manager offices for safeguarding purposes.

9 Security

- **Control room:** The Main Office is the control room and is accessible only to Headteacher, Office Manager, and the Facilities Team. Casual access is prohibited; contractors must be verified and recorded.
- **Access controls:** System access is password-protected and restricted to authorised staff. Authorised operators include the Headteacher, Office Manager and Facilities Team. Teachers may be authorised by the Headteacher to view footage for a specific event and purpose; the Headteacher may authorise additional roles on a documented, case-by-case basis.
- **Security assurance:** The system will be subject to periodic security testing; faults will be rectified promptly to minimise data protection risk. Visual display monitors are located only in designated secure areas.
- **Covert surveillance:** Only in exceptional, proportionate circumstances and with appropriate RIPA authorisation retained on file.

- **Data breaches:** Any actual or suspected data breach involving CCTV footage (including unauthorised access, loss, or disclosure) must be reported immediately to the Headteacher and DPO in accordance with the school's Data Breach Response Procedure. Where a breach meets the threshold under UK GDPR Article 33, the ICO will be notified within 72 hours. Where there is a high risk to individuals, affected data subjects will be notified in accordance with Article 34.

10 Retention and evidence handling

- **Default retention:** Recorded images are retained for six (6) days) unless required longer for a specific incident, investigation or legal process, in which case they are retained only for as long as necessary for that purpose.
- **Evidence export:** Where footage is required as evidence, authorised staff will export a copy to a uniquely identified, tamper-evident medium (e.g., write-once media or secure digital export) with an accompanying evidence log, and store it securely. Historical Clapham and Patching practice of sealing numbered discs and secure disposal is maintained where physical media are used.
- **Secure disposal:** When no longer required, exported media will be securely destroyed.

11 Privacy by Design (DPIA)

A Data Protection Impact Assessment (DPIA) has been completed for the current CCTV deployment and is held on file. A further DPIA will be completed before any new CCTV installation, change in purpose, significant camera repositioning, or introduction of audio recording. Note: audio is **not** currently recorded by any camera in this system.

Where high risk to individuals cannot be mitigated, Clapham and Patching will consult the ICO before proceeding and act on the ICO's advice.

12 Code of Practice

- Clapham and Patching understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- The school notifies all pupils, staff and visitors of the purposes for which CCTV data is collected through: CCTV warning signs at all access points; the school's Privacy Notice (published on the school website and available on request), which includes a dedicated section covering CCTV processing, lawful basis, retention, and individual rights; and, where applicable, direct communication with staff and families. The Privacy Notice fulfils the transparency requirements of UK GDPR Articles 13 and 14.
- CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- All surveillance footage will be retained for a default period of six days, in accordance with the retention schedule in section 10. Retention beyond this period is only permitted where footage is required for an ongoing incident, investigation or legal process, in which case it is retained only for as long

as necessary for that purpose. The Headteacher and the Data Controller are responsible for keeping records secure and managing access.

- The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.
- The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.
- The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the school's website.

The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point through which people can access information and submit complaints.
- Have clear responsibility and accountability procedures for images and information collected, held and used.
- Have defined policies and procedures in place which are communicated throughout the school.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access.
- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up-to-date.

13 Access (Subject Access Requests & Disclosure)

Subject Access Requests (SARs): Individuals have the right to request access to personal data in CCTV images. Clapham and Patching will verify identity and respond within one month; a reasonable fee may be charged for repetitive/excessive requests or additional copies. Requests should be addressed to the Headteacher/DPO.

Third-party disclosure: Release of images is restricted and recorded. Disclosures may be made only to: the police (for a specific criminal inquiry), prosecution agencies (e.g., CPS), relevant legal representatives, or the data subject where entitled under data protection and FOI law. The Headteacher makes the final decision on any disclosure to persons other than the police.

Media: Images will not be released for entertainment or commercial purposes.

14 Monitoring and Review

The Headteacher monitors legislative updates and ensures the policy and practice remain compliant; material changes are communicated to staff.

Formal review: every 3 years (see Document Control), or earlier if there are significant legal or operational changes.

15 Equality, Safeguarding and Data Protection Statement

Clapham and Patching will ensure the operation of CCTV respects the rights and dignity of individuals, is non-discriminatory, and supports safeguarding. Data protection principles apply in full, and any privacy risks are assessed and mitigated through DPIA.

16 Contact

- Data Controller (day-to-day): CFOO, Clapham and Patching
- Headteacher: Clapham and Patching
- DPO: SchoolPro (on behalf of Clapham and Patching)

17 Appendix A (informative): Typical camera locations (high-level)

- External: site perimeter, entrances, car parks.