Closed-Circuit Television Policy

1. Policy Statement. The Queen's College operates a Closed-Circuit Television (CCTV) system to support the safety, security, and lawful management of its premises. The system is operated in accordance with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, and the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012. The College recognises that CCTV data constitutes personal data where individuals are identifiable and will process such data lawfully.

2. Purpose of CCTV. The College has installed CCTV for the following defined purposes:

- Protection of students, staff, visitors, and contractors.
- Prevention and detection of crime and anti-social behaviour.
- Protection of College property and assets.
- Assistance in the investigation of incidents.
- Supporting health and safety compliance.

CCTV will not be used for routine staff performance or student behavioural monitoring.

3. Lawful Basis for Processing. Processing of CCTV data is carried out under the following lawful bases:

- Article 6(1)(c) UK GDPR – Compliance with legal obligation.
- Article 6(1)(f) UK GDPR – Legitimate interests of the College.

Where special category data is incidentally captured, processing will comply with Article 9 UK GDPR and Schedule 1 of the Data Protection Act 2018. A Legitimate Interests Assessment (LIA) will be maintained where required.

4. System Operation and Management. The CCTV system is owned and controlled by The Queen's College. The Head Porter - supported by the IT Manager - is responsible for:

- Authorising access to recordings.
- Ensuring compliance with legal obligations.
- Oversight of system operation.
- Maintaining access logs.
- Initiating an annual review of system necessity and proportionality through the College Security Working Group.

The system will:

- Be positioned to minimise intrusion into private areas.
- Not record in toilets, changing rooms, prayer rooms, or other private spaces.
- Operate continuously unless otherwise stated.

Audio recording is not enabled unless specifically authorised by the DB and documented.

5. Access to recordings. On-duty Porters have daily access to live camera feeds. In addition, the Deputy Librarian has access to live coverage of the library building when lone working in the evenings.

Access to recorded footage is limited to:

- Head Porter and Deputy Head Porter.
- Bursar, Domestic Bursar, Deputy Domestic Bursar (where relevant to investigations).
- LSO and the Tutor for Welfare (where relevant to investigations).
- Deputy Librarian (where relevant to investigations).
- IT Manager and Systems Officer for technical maintenance only (do not carry out investigations).

External access may be granted to:

- Law enforcement agencies upon formal request.
- Regulatory bodies where legally required.

All access requests must:

- Be documented.
- State purpose, together with date and time under investigation.
- Be approved by Head Porter in consultation with Domestic Bursar.
- Be logged in an Access Register.

Unauthorised viewing, copying, downloading, or sharing of footage is prohibited and may constitute gross misconduct.

6. Storage and Retention.:

- CCTV recordings are stored on a physical CCTV server located in secure location.
- Footage is protected by password restrictions.
- Footage is retained for a maximum of 30 days, then automatically deleted.

Footage required for investigation, legal proceedings, safeguarding, or disciplinary action may be retained longer, with documented justification. Investigation footage will be deleted manually once investigations are complete[1].

7. Disclosure of Footage. Disclosure of CCTV footage will occur only where lawful and proportionate. Requests must be:

- Submitted in writing.
- Assessed for data protection compliance.
- Approved by the Head Porter in consultation with Domestic Bursar (or delegates).

Individuals may request access under Subject Access Request (SAR) procedures. Still images of third-parties will be redacted where necessary.

8. Signage Requirements. Clear signage is displayed:

- At all entrances to College premises.
- At key monitored areas.
- In a visible, legible format.

Signage includes:

- Notification that CCTV is in operation.
- The purpose of monitoring.
- The identity of the data controller (The Queen's College).
- Contact details for further information.

Signage will be reviewed during the annual ACOP audit to confirm visibility, condition, and accuracy.

9. Policy Review and Audit. The CCTV system and this policy will be reviewed by the College Security Working Group annually or sooner if:

- System changes occur.
- New legal requirements arise.
- Complaints or breaches are identified.

The review will confirm:

- The continued necessity and proportionality of CCTV.
- That the purpose of CCTV remains valid.
- That access controls remain appropriate.
- That retention periods are justified.
- That signage remains compliant and visible

[1] Although we will preserve records until the limitation periods for legal action have elapsed.

Findings will be documented.

10. Data Security. Appropriate technical and organisational measures are implemented, including:

- Password protection.
- Restricted administrator rights.
- Secure physical server location.
- Access logs.

Any data breach involving CCTV will be managed in accordance with the College Data Breach Policy.

11. Training. The Head Porter will arrange training for staff with access to CCTV covering:

- Data protection obligations.
- Confidentiality requirements.
- Appropriate disclosure.
- Incident handling procedures.

12. Complaints. Complaints relating to CCTV use should be made to the DPO.

13. Responsibility. The Governing Body (through the Bursar and Domestic Bursar) hold overall accountability for compliance. Operational responsibility rests with the Head Porter in consultation with the IT Manager.

This policy is effective from March 2026 and supersedes all previous CCTV policies.