



CCTV and ANPR Policy

Policy Statement

St Edmund's College ("the College") operates Closed-Circuit Television (CCTV) and Automatic Number Plate Recognition (ANPR) systems to help protect people, property and information, and to support the safe and effective running of the College.

The College will ensure that all CCTV and ANPR use is lawful, fair, transparent, necessary and proportionate, and complies with the UK General Data Protection Regulation (GDPR), Data Protection Act 2018 (DPA), the Surveillance Camera Code of Practice and Article 8 of the European Convention on Human Rights (ECHR) (right to respect for private and family life).

The College recognises that CCTV and ANPR may affect individuals' privacy and will therefore use them only for clearly defined purposes, limit their intrusiveness, inform individuals about their use, and maintain appropriate governance and oversight.

This Policy is binding on all members of St Edmund's College and employees of contracted-out services, and applies to all other persons present on College property.

1. Purpose

This Policy sets out the purposes, scope and governance arrangements for the CCTV and ANPR systems operated by the College.

It is intended to ensure that CCTV and ANPR are used in a way that:

- Is necessary and proportionate;
- Complies with UK GDPR and DPA 2018;
- Has regard to the Surveillance Camera Code of Practice; and
- Respects the rights and freedoms of individuals.

2. Scope

This Policy applies to:

- All CCTV and ANPR systems owned, managed or operated by the College on any College premises or land;
- All staff of the College, contractors and any third parties who have authorised access to the CCTV systems; and
- All individuals whose images or related information are captured by the systems while on, or in the immediate vicinity of, College property.

This Policy is binding on all members of St Edmund's College and employees of contracted-out services. It also applies to all other persons who may be present, for whatever reason, on College property.

3. Legal and Regulatory Framework

The College operates CCTV and ANPR in accordance with, in particular:

- UK GDPR and DPA 2018;

- the Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice;
- the Human Rights Act 1998 (Article 8 ECHR); and
- guidance issued by the Information Commissioner’s Office (ICO) on CCTV, video surveillance and ANPR.

This Policy should be read in conjunction with the College’s Data Protection Policy. For data protection purposes, the College is the Data Controller for personal data captured by CCTV and ANPR systems.

4. Principles

The College will ensure that its CCTV and ANPR systems are:

- Operated fairly, lawfully and transparently;
- Used only for specified, explicit and legitimate purposes;
- Necessary and proportionate to meet those purposes;
- Subject to appropriate technical and organisational security measures; and
- Subject to appropriate governance, accountability and review, including Data Protection Impact Assessments (DPIAs) where required.

The systems are operated as overt surveillance, using visible cameras. Covert monitoring will only take place in exceptional circumstances, for a strictly limited period, where authorised in accordance with law and College procedures (i.e. where necessary for the prevention or detection of serious crime and where overt monitoring would prejudice that purpose).

The College does not use the CCTV or ANPR systems for automated decision-making or profiling and does not use facial recognition or similar biometric identification technologies. If this position changes, a DPIA will be completed and this Policy updated before such technologies are deployed.

5. System Description

The College’s CCTV system comprises approximately 90–100 overt colour motion-sensing cameras located primarily in public or semi-public areas of the main and ancillary sites (including entrances, circulation spaces, and areas requiring heightened security such as storage rooms and plant rooms).

Live images from cameras are displayed on monitors located on the staff side of the Porters’ Lodge. Images are recorded onto secure digital storage located either per site, per building or per camera, as appropriate.

Select cameras can detect and record Vehicle Registration Marks (VRMs) using Automatic Number Plate Recognition (ANPR) to support management and monitoring of College roads and car parks.

The systems do not normally record audio. Any limited audio capability will be disabled unless expressly justified, subject to a DPIA and clearly signposted in advance.

Cameras are installed and configured so as not to intrude into private domestic areas, including neighbouring residential properties.

6. Purpose of CCTV and ANPR

The primary purposes of the systems are to:

- Detect, prevent or reduce the incidence of crime and antisocial behaviour;

Version No: 2	Version Date: January 2026	Policy Owner: Governance, Risk & Compliance Manager
----------------------	-----------------------------------	--

- Protect the safety and security of students, staff, Fellows, visitors, contractors and members of the public;
- Protect College buildings, assets and information;
- Assist in the investigation of suspected offences or disciplinary matters;
- Assist in the effective management of emergencies and incidents;
- Provide assistance to the emergency services;
- Support health and safety (e.g. investigating accidents or near-misses);
- Monitor use of College roads and car parks, including ANPR for parking management and enforcement;
- Reduce the fear of crime and help create a safer College community; and
- Gather evidence by a fair and accountable method.

CCTV may also be used to live-stream and/or record selected events held in College function rooms or spaces for public or private viewing, where this is compatible with data protection requirements and appropriate notice has been given.

These purposes will be reviewed at least every two years to ensure continued necessity and proportionality.

7. Governance, Accountability and DPIAs

The Bursar is the Senior Responsible Officer for CCTV and ANPR and overall compliance with this Policy.

Day-to-day operational responsibility is delegated to the Domestic Bursar in conjunction with the Governance, Risk & Compliance Manager who acts as the College's Data Protection Lead (CDPL).

A DPIA will be conducted and kept under review for the CCTV system as a whole, for ANPR processing, and for any significant changes (new cameras, locations, technologies or purposes).

8. Fairness, Transparency and Signage

The College will provide clear and prominent signage at entrances to sites, buildings and car parks and in other locations as appropriate.

Signs will indicate that CCTV and/or ANPR monitoring and recording is in operation, identify the College as system operator, state the main purposes, and provide contact/further information.

The CCTV and ANPR Policy will be published on the College website, explaining purposes, legal bases, retention, recipients, individuals' rights and contact details.

9. Legal Basis for Processing

The College will normally process personal data captured through CCTV and ANPR on the basis that it is necessary for:

- Performance of tasks carried out in the public interest or in the exercise of official authority (Article 6(1)(e) UK GDPR); and/or
- Legitimate interests pursued by the College or a third party (Article 6(1)(f) UK GDPR), such as crime prevention, property protection and parking management, where these interests are not overridden by the rights and freedoms of the individuals concerned.

Where footage captures criminal offence data, the College will ensure compliance with Article 10 UK GDPR and the relevant provisions of Schedule 1 DPA 2018.

10. Access to Live Footage

With the exception of authorised live-streamed events, live footage can only be monitored in the Porters' Lodge. Only designated College staff, trained in their duties and in this Policy, may monitor live footage. Access to the Porters' Lodge, monitors and controls is restricted to authorised personnel.

Monitoring must be purpose-limited and not used for inappropriate observation where no legitimate purpose exists.

11. Access to Recordings (Internal)

Only designated staff (e.g. the Head Porter, Senior Porters, Head of Facilities & Accommodation, IT Manager) may have primary access to CCTV and ANPR recordings for operational purposes and in accordance with section 6.

The Bursar (or nominee) must authorise access to recordings by other specific College staff where necessary for crime prevention, serious disciplinary matters, health and safety investigations, apprehension or prosecution of offenders or matters of national security.

All access to recordings (viewing, copying, export) will be logged, including date/time, identity and role of person accessing, purpose, camera(s) and date range, and details of any onward disclosure.

12. Disclosure to Third Parties (including Police)

The College may disclose recordings to the police or other law enforcement / regulatory bodies where this is necessary and lawful (e.g. for prevention/detection of crime, apprehension or prosecution of offenders, or protection of vital interests).

Where the College initiates contact with the police, designated staff may release footage where there is a reasonable belief it will assist the investigation and a lawful basis for disclosure exists.

Where the police or another official body request access, they will normally be asked to provide a written request confirming the legal basis and necessity of the request.

Any other request (e.g. insurers, legal representatives) will be referred to the Bursar and DPO.

All external disclosures will be logged and, where appropriate, copies controlled (e.g. watermarked), and recipients reminded of their responsibilities as independent Data Controllers.

13. Data Subject Rights and Access by Individuals

Recordings that identify, or are reasonably likely to identify, a living individual are personal data. Individuals have qualified rights, including to be informed, access, rectification, erasure, restriction, objection and complaint to the ICO.

Requests to exercise these rights in relation to CCTV or ANPR (including Subject Access Requests for footage) should be made to the CDPL using the contact details on the College website. Requests may also be routed via the Bursar.

The College will respond within the timescales set by law, subject to applicable exemptions and the need to protect the rights and freedoms of others (e.g. where third parties are visible).

The College may ask for further information to locate footage, and may blur/obscure third parties or explain where footage cannot be provided (e.g. overwritten or exempt).

14. Retention of recorded materials and disposal

CCTV and ANPR recordings will be retained no longer than necessary.

Routine recordings will normally be retained for no more than 30 days, after which they will be overwritten or securely deleted unless flagged or exported in connection with an ongoing incident or investigation.

Where footage is retained for an incident, it will be kept only as long as necessary, in line with the College's Records Retention Schedule, and in any event normally no longer than three years from the date of recording unless there is a clear legal requirement to retain it longer.

All media or storage containing recordings that are no longer required will be securely erased or destroyed in accordance with College information security procedures.

15. ANPR-Specific Provisions

ANPR cameras capture VRMs and may also capture images of drivers and pedestrians. When linked to identifiable individuals, VRMs are personal data.

The use of ANPR will be explicitly covered in relevant DPIAs, including assessment of necessity, proportionality, privacy risks and mitigation.

ANPR data will only be used for:

- Monitoring and enforcing compliance with College parking policy;
- Investigating misuse of College roads and car parks;
- Supporting security investigations;
- Compliance with legal obligations (e.g. lawful requests from enforcement bodies).

ANPR records will be retained and disclosed in line with sections 13 and 15 and the relevant privacy notice.

16. Live-Streaming and Recording of Events

The College may use CCTV or related equipment to live-stream or record events (e.g. lectures, ceremonies, public talks).

Event organisers must ensure attendees are informed in advance that recording or live-streaming will take place and for what purposes, and that the lawful basis and retention period are clear and compatible with this Policy. Where reasonably practicable, areas should be provided for individuals who do not wish to be filmed.

Event recordings will be stored, shared and archived in line with the College's records management and data protection policies.

17. Security, System Management and Training

Systems will be protected by appropriate technical and organisational security measures, including user access controls, role-based permissions, secure configuration, patching, secure storage and secure disposal.

Only trained and authorised personnel may configure equipment, manage access or export/copy/download footage.

Staff with responsibilities under this Policy will receive appropriate training on the legal framework, the Surveillance Camera Code, privacy and data protection, and information security/incident reporting.

18. Breaches, Misuse and Complaints

Any suspected misuse of CCTV or ANPR, or breach of this Policy, must be reported promptly to the Bursar and/or the Governance, Risk and Compliance Manager.

Breaches may be dealt with under relevant disciplinary procedures. Serious or deliberate misuse may constitute gross misconduct and may also result in criminal liability.

Where appropriate, the College will consider referring matters to the police or other authorities.

A copy of this Policy will be made available on request and via the College website.

Individuals with concerns or complaints should raise them in the first instance with the Bursar or Governance, Risk & Compliance Manager. If still dissatisfied, they may complain to the Information Commissioner's Office (ICO).

19. Review

This Policy, and the operation of CCTV and ANPR systems, will be reviewed every two years, and sooner if there are significant changes to systems, law, guidance or in response to incidents or complaints.