



CLOSED CIRCUIT TELEVISION (CCTV) POLICY

This policy adheres to and should be applied with due consideration to the College's commitment to the Framework for Ethical Leadership in Education.

This policy has been reviewed in line with the Sustainable Development Goals.

Mission Statement

Our mission inspired by the Christian tradition is to be a community based on faith, hope and love; developing each individual intellectually, emotionally and spiritually to achieve their full potential. To achieve this we will:

- Provide a welcoming, supportive community where everyone is valued.
- Provide a high quality, meaningful education which encourages the development of the whole person, inspired by the Notre Dame tradition.
- Promote a caring environment, rooted in the virtues of service, kindness, gratitude and respect.
- Work together for the benefit of each person as well as the wider community.
- Recognise, celebrate and treasure, without exception, the unique gifts and dignity of each person, ensuring equality and fairness for all, as found in the teaching and example of Our Lord Jesus Christ.
- Comprehensive updated draft incorporating governance, safeguarding, GDPR, access control, retention, maintenance and review requirements.

Version	4
Author	Capital Projects and Estates Manager
Date Reviewed	September 2026
Approved by SLT	September 2026
Approved by Full Corporation	October 2026
Review Interval	1 year
Previous Review Date	September 2025
Next Review	September 2027

PURPOSE

The College operates CCTV to protect students, staff, visitors, contractors and assets; support safeguarding, safety and security investigations; deter and detect crime; and assist emergency response.

The College recognises that CCTV systems are a valuable component of wider safeguarding, security and health and safety arrangements, but are only one part of a broader risk management framework. The College operates a digital networked CCTV system comprising internal and external cameras located across the estate. The system is designed to support safeguarding, security, operational management and incident investigation.

Legal Framework

UK GDPR, Data Protection Act 2018, Human Rights Act 1998, Freedom of Information Act 2000, Protection of Freedoms Act 2012, ICO guidance and KCSIE.

Scope

This policy applies to all CCTV systems owned, operated or managed by the College. It applies to employees, students, governors, contractors, visitors and any other individuals who may be recorded on College premises.

Lawful Basis for Processing

The College processes CCTV data under the lawful basis of Legitimate Interests and, where applicable, Public Task in accordance with UK GDPR and the Data Protection Act 2018.

ROLES AND RESPONSIBILITIES

Governors

- Strategic oversight of the CCTV system.
- Receiving assurance that CCTV remains lawful, proportionate and effective.
- Ensuring the College meets its legal and regulatory obligations.

Principal

- Overall accountability for CCTV operation.
- Authorisation of external disclosures.

Capital Projects and Estates Manager

- Management of CCTV assets.
- Annual CCTV reviews.
- Coordination of maintenance contracts.
- Reviewing camera locations.
- Management of CCTV signage.
- Supporting investigations.
- Fault management.
- Maintaining records of CCTV system upgrades, maintenance and replacement planning.

IT Manager

- Security of CCTV infrastructure.
- User permissions.
- Password management.
- System backup and resilience.

Data Protection Officer

- GDPR compliance.
- Subject Access Requests.
- Data sharing advice.
- Data Protection Impact Assessments.

Designated Safeguarding Lead

- Safeguarding investigations.
- Review of safeguarding footage.
- Liaison with external safeguarding agencies.

CCTV LOCATIONS AND USE

CCTV Locations

The College operates a network of CCTV cameras at strategic locations across the estate to support safeguarding, security, health and safety and operational requirements. Camera locations are determined following consideration of risk, operational need and the privacy rights of individuals.

- CCTV cameras may be installed in locations including:
- Main entrances and exits.
- Reception areas.
- Internal circulation spaces and corridors.
- Stairwells.
- Student communal areas.
- Car parks and vehicle access points.
- External pedestrian routes and pathways.
- Sports facilities.
- Building perimeters and service areas.
- Other locations identified through risk assessment or security review.

Use of CCTV

The College uses CCTV systems for the following purposes:

- Protecting the safety and wellbeing of students, staff, visitors and contractors.
- Supporting safeguarding and welfare investigations.
- Preventing and detecting crime, anti-social behaviour and vandalism.
- Protecting College buildings, equipment and assets.
- Assisting investigations into accidents, incidents and near misses.
- Supporting health and safety management.
- Assisting emergency response and business continuity arrangements.
- Managing site security and controlling access to College premises.

- Supporting investigations into alleged breaches of College policies and procedures.
- Providing evidential material where required by authorised agencies.

Privacy Considerations

The College is committed to operating CCTV systems in a lawful, proportionate and transparent manner.

Cameras shall be positioned to minimise intrusion into areas where privacy may reasonably be expected. CCTV systems will not normally monitor neighbouring properties, public spaces unrelated to College activities or private areas without clear justification.

Under no circumstances will CCTV cameras be installed in:

- Toilets.
- Changing rooms.
- Shower facilities.
- Medical treatment rooms.
- Any other area where individuals would have a reasonable expectation of privacy.

Any proposal to install additional cameras or significantly alter existing camera coverage shall be subject to review by the Capital Projects and Estates Manager and, where required, a Data Protection Impact Assessment (DPIA) to ensure compliance with UK GDPR and the Data Protection Act 2018.

Review of Camera Locations

The Capital Projects and Estates Manager shall review CCTV coverage periodically and as part of the annual CCTV system review to ensure that camera locations remain necessary, proportionate and effective in meeting the College's safeguarding, security and operational objectives.

CCTV Signage

Appropriate CCTV signage shall be displayed at site entrances and other relevant locations to inform individuals that CCTV is in operation.

Signage shall identify the College as the Data Controller and provide information on how further information can be obtained regarding the operation of the CCTV system.

Access Controls

Access restricted to authorised personnel through individual user accounts. Passwords must be protected and access reviewed periodically.

System Management and Monitoring

The College operates CCTV primarily as a retrospective investigative tool. CCTV footage is not routinely monitored continuously.

Live monitoring and retrieval of footage shall only be undertaken by authorised personnel where there is a legitimate safeguarding, security, operational, health and safety or business continuity purpose.

All access to live or recorded footage shall be proportionate and undertaken only where there is a legitimate operational need.

CCTV Asset Management

The Capital Projects and Estates Manager shall maintain a CCTV asset register including:

- Camera locations.
- Network video recorders and storage devices.
- Maintenance records.
- Fault reports.

System upgrades and modifications.

CCTV assets shall be included within the College's Planned Preventative Maintenance Programme and asset replacement planning process.

Safeguarding

CCTV may be used to support safeguarding investigations. Access shall be restricted to staff with a legitimate operational need.

Fault Reporting

Any fault affecting CCTV operation, image quality, recording functionality or storage shall be reported to the Capital Projects and Estates Manager as soon as reasonably practicable.

Faults shall be logged, investigated and prioritised according to the associated risk.

If faults could significantly affect safeguarding or security arrangements, interim control measures shall be considered until repairs are completed.

Use in Investigations

CCTV footage may be used to support:

- Safeguarding investigations.
- Student disciplinary investigations.
- Staff investigations.
- Health and safety investigations.
- Criminal investigations.
- Insurance claims.
- Investigations into breaches of College policies and procedures.

All reviews of footage must be proportionate, necessary and relevant to the matter being investigated.

Subject Access Requests and Individual Rights

Individuals may request access to CCTV footage containing their personal data through a Subject Access Request in accordance with the Data Protection Act 2018 and UK GDPR.

Requests shall be managed by the Data Protection Officer and in accordance with statutory timescales and the College Data Protection procedures.

The College may redact, withhold or restrict disclosure where disclosure would adversely affect the rights and freedoms of other individuals or where another lawful exemption applies.

Disclosure of Footage

CCTV footage may be disclosed where there is a lawful basis to do so, including:

- Requests from the Police.
- Court Orders.
- Insurance investigations.
- Regulatory investigations.
- Safeguarding investigations involving external agencies.

All disclosures shall be authorised by the Principal, Data Protection Officer, Designated Safeguarding Lead, or Capital Projects and Estates Manager (as appropriate), recorded where necessary, and comply with data protection legislation.

Retention

CCTV footage will normally be retained for 30 days before being automatically overwritten. Footage required for safeguarding matters, investigations, disciplinary processes, insurance claims or legal proceedings may be retained for longer where justified and appropriately authorised.

Data Security Incidents

Any actual or suspected unauthorised access, disclosure, loss, corruption or misuse of CCTV footage shall be reported immediately to the Data Protection Officer.

Incidents shall be managed in accordance with the College Data Protection and Data Breach procedures.

Third Party Access

External contractors or service providers may be granted access to CCTV systems where necessary to support installation, maintenance, repairs or technical support.

Such access shall be appropriately controlled, authorised and limited to the minimum necessary for the task being undertaken.

Where personal data may be accessed, appropriate contractual and data protection controls shall be in place.

Maintenance and Review

Routine inspections, recording checks, date and time verification, equipment testing and annual effectiveness reviews will be undertaken.

The annual review shall consider:

- Ongoing operational need for CCTV.

- Camera effectiveness and coverage.
- System reliability and fault history.
- Requests for footage and Subject Access Requests.
- Complaints relating to CCTV operation.
- Safeguarding and security trends.
- Compliance with data protection legislation.
- Requirements for additional cameras or relocation of existing cameras.

This policy shall also be reviewed following:

- Significant safeguarding incidents.
- Major changes to the CCTV system.
- Changes in legislation, ICO guidance or best practice.
- Recommendations arising from audits or inspections.
- Significant alterations to the College estate.