ST. JOSEPH'S COLLEGE
READING • BERKSHIRE

CCTV Policy

Policy Owner Bursar	Associated documents Data Protection Policy for Pupils and Parents Data Protection Policy for Staff Privacy Notice for Staff, Parents and Alumni Privacy Policy for Students	Legal Framework
Review by SLT	Review frequency Every 3 years	Next Reviewed date April 2028

ST. JOSEPH'S COLLEGE
READING • BERKSHIRE

St. Joseph's College CCTV Policy

1. Purpose of the Policy

This policy regulates the management, operation, and use of the Closed-Circuit Television (CCTV) system at St. Joseph's College. It aims to:

- Protect the safety of pupils, staff, volunteers, and visitors.
- Safeguard College property and personal belongings.
- Support law enforcement and community safety efforts.
- Ensure compliance with data protection laws (GDPR).
- Establish clear guidelines for authorised access and use.

2. Scope

This policy applies to all sections of St. Joseph's College, including the Early Years Foundation Stage, and covers all CCTV equipment and footage managed by the College.

3. Roles and Responsibilities

- **Data Controller**: St. Joseph's College.
- **Data Protection Lead (DPL)**: Responsible for ensuring compliance with data protection laws.
- **Bursar & Estates Bursar**: Oversee the day-to-day management of the CCTV system.
- **IT Department**: Responsible for the administration, maintenance, and technical support of the CCTV system, including remote access.

4. Authorised Personnel

- Only the following personnel are authorised to access and operate the CCTV system:
    - **Estates Bursar & Bursar**
    - **IT Department (Head of IT Strategy, IT Support Staff)** for system maintenance, troubleshooting, network management and assisting with footage
    - **Designated Safeguarding Lead (DSL)** for safeguarding and behavioural concerns.
    - **Deputy Head (Senior)** for behavioural concerns.
    - **Compliance Manager** for audit and compliance purposes.
    - **Other authorised personnel** as approved by the Bursar.

5. CCTV System Overview

- The College uses the **Unifi Protect System**, including fixed cameras, which are positioned in key areas to fulfil the objectives outlined in this policy.
- Cameras are in plain sight, with signage indicating CCTV monitoring.
- No cameras are installed in areas with an expectation of privacy (e.g., changing rooms, toilets, swimming pool).
- Cameras are permanently muted and do not record audio

6. Access from Non-College Devices

- **Remote Access**: Authorised IT personnel may access the CCTV system remotely using secure methods, such as:
    - VPN (Virtual Private Network) and multi-factor authentication.
    - Approved devices only (College-issued laptops or personal devices with enhanced security protocols).
    - Remote access is permitted solely for troubleshooting, maintenance, urgent security issues, and approved investigations.
- **Personal Devices**: IT staff may use personal devices for remote access when necessary, provided security measures are in place to protect data integrity and privacy.

7. Usage Guidelines

- **Maintenance and Troubleshooting**:
    - The IT department is authorised to access CCTV footage for technical support, including network diagnostics, camera maintenance, and firmware updates.
    - Regular checks are performed to ensure cameras are operational, free from obstructions, and correctly positioned.
- **Incident Investigation**:
    - CCTV footage may be accessed for investigations relating to safeguarding, security breaches, or incidents involving pupils, staff, or property damage.
    - Requests for footage must be directed to the IT department, Bursar or DSL. The relevant staff will verify the purpose of the request and direct it to the appropriate authority (DSL/Deputy Head Senior for pupil matters, HR for staff matters, Estates for facilities).
- **Data Retention**:
    - Footage is stored securely for up to **14 days** unless needed for ongoing investigations or legal proceedings.

- Any access to footage must be logged, detailing the person accessing, date, time, and purpose.

8. Monitoring and Data Security

- CCTV footage is monitored in secure areas, including:
  - Bursary Office – Front Entrance and Reception
  - IT Office (Support Office) – All cameras
  - Prep Office – Prep Gate
  - Estates Bursar's Office
- **Access Control**: Access to CCTV monitors and footage is restricted to authorised personnel only.
- **Data Protection Compliance**:
  - All staff with access to the CCTV system must undergo training on GDPR compliance and data protection.
  - Regular audits are conducted by the Compliance Manager to ensure adherence to this policy.

9. Request for CCTV Footage

- **Internal Requests**:
  - Staff requesting access to footage must provide a clear reason. Requests will be evaluated based on their relevance to the College's objectives (safeguarding, security, maintenance).
  - The IT department will log all requests and redirect them to the appropriate authority for approval.
- **External Requests**:
  - Requests from law enforcement or other external entities must be approved by the Bursar or the Data and Compliance Manager.
  - The requesting entity must complete a data request form and return this to the Data and Compliance Manager before footage can be provided.
  - Where possible, non-relevant individuals' faces will be obscured before footage is shared.

10. Breach of Policy

- Unauthorised access, use, or disclosure of CCTV footage is strictly prohibited and may result in disciplinary action, up to and including termination of employment.
- Incidents of misuse will be investigated, and corrective actions will be taken to prevent future occurrences.

11. Policy Review

- This policy will be reviewed annually, or earlier if significant changes to the CCTV system or data protection laws occur. The next scheduled review is **April 2026**.
- The Head of IT Strategy, Bursar, and Data and Compliance Manager will jointly conduct the review to ensure the policy remains relevant and up-to-date.

12. Complaints and Queries

- Any complaints or queries regarding the CCTV system should be directed to the Bursar.
- Individuals may request access to footage involving them by submitting a formal request to the Data Protection Lead, including details such as date, time, and camera location.

CCTV Procedures

1. Purpose

This document provides detailed instructions for accessing, maintaining, and using the CCTV system at St. Joseph's College, in compliance with the College's CCTV Policy and GDPR.

---

2. Accessing CCTV Footage

Step 1: Request Submission

1. The requester must submit a support ticket to the IT Department using techsupport@sjcr.org.uk which will generate a support ticket.
2. The request must include:
    - Name and contact details of the requester.
    - Specific date, time, and camera location of the footage requested.
    - Purpose of the request (e.g., safeguarding, incident investigation, intruder, estates issue).
    - Level of urgency

Step 2: Verification and Authorisation

1. The IT Department will verify:
    - The requester's identity.
    - The legitimacy of the request as aligned with policy objectives.
2. Authorisation will be obtained from:
    - **DSL or Deputy Head (Senior)** for student-related matters.
    - **Head or Bursar** for staff-related matters.

- **Estates or Data and Compliance Manager** for property or operational issues.

Step 3: Access and Disclosure

1. Approved access to footage will be logged in the helpdesk system, including:
    - Date and time of access.
    - Name of the individual accessing the footage.
    - Purpose of the request.
2. If footage is shared externally (e.g., police), the IT Department will ensure:
    - Non-relevant individuals' identities are obscured where feasible.
    - A record is kept of all disclosed footage, including the recipient's details.

---

3. Maintenance and Troubleshooting

Regular Maintenance

1. IT staff will:
    - Check cameras for obstructions (e.g., cobwebs, physical damage).
    - Verify camera alignment and functionality.
    - Perform firmware updates on the **Unifi Protect** system.
    - Monitor storage capacity to ensure proper data retention.

Troubleshooting

1. For network or technical issues, IT will:
    - Use CCTV to check door operations, network connectivity, or camera activity.
    - Document and resolve identified issues promptly.
    - Notify relevant departments if a problem impacts operations.

---

4. Remote Access

Permitted Use

1. Remote access to the CCTV system is restricted to authorised IT staff for:
    - Urgent troubleshooting or maintenance.

- Incident investigations requiring immediate attention.

Security Protocols

1. Remote access must use:
    - **VPN** for a secure connection.
    - **Multi-factor authentication** for system login.
    - Approved devices (College-issued or secured personal devices).
2. Remote access logs must record:
    - The date and time of access.
    - The purpose of access.
    - The individual accessing the system.

---

5. Data Breach or Misuse Response

1. Any suspected misuse of the CCTV system must be reported to the Data and Compliance Manager immediately.
2. The IT Department will:
    - Suspend access for the individual involved (if applicable).
    - Investigate and document the incident.
3. Findings will be reviewed by the Head and/or Bursar and appropriate action taken.

CCTV Processes Document

1. Incident Investigation Process

Objective: To outline the workflow for investigating incidents using CCTV footage.

Steps:

1. **Incident Detection**:
    - Incident reported by staff, student, or system alert.
    - Notify the DSL, Deputy Head (Senior), Estates, or IT department, depending on the nature of the incident.
2. **Request for Footage**:
    - Submit a **ticket to techsupport**@sjcr.org.uk
    - Verify the legitimacy of the request.

3. **Review Footage**:
    - IT staff retrieve relevant footage.
    - Review footage with authorised personnel present (e.g., DSL for safeguarding).
4. **Action Taken**:
    - Use footage to support decisions (e.g., pupil investigation, disciplinary action, police involvement).
    - Document findings and outcomes in the helpdesk ticket.
5. **Follow-Up**:
    - Ensure all footage related to the incident is securely retained for legal or administrative purposes.
    - Notify involved parties of outcomes as appropriate.

---

2. Maintenance Workflow

Objective: To ensure the CCTV system remains fully operational.

Steps:

1. **Weekly Checks**:
    - IT conducts visual inspections of cameras.
    - Confirm alignment, clarity, and operational status.
2. **Monthly Maintenance**:
    - Perform firmware updates.
    - Clear obstructions or reposition cameras as needed.
    - Test recording and storage functionality.
3. **Issue Resolution**:
    - Use the CCTV system to diagnose problems (e.g., door not unlocking).
    - Escalate unresolved issues to external vendors (if required).

---

3. Request Handling Process

Objective: To streamline requests for CCTV access or footage.

Steps:

1. **Submit Request**:

- Form completed by the requester and submitted to IT or the Bursar.

2. **Verify**:
   - IT checks the form for completeness and confirms the requester's identity.
3. **Authorisation**:
   - Obtain sign-off from the appropriate authority (e.g., DSL, Deputy Head (Senior), HR, Estates).
4. **Grant Access or Share Footage**:
   - Footage accessed under supervision or shared securely with necessary documentation.
5. **Log Entry**:
   - Record details of the request, access, and disclosure in the CCTV log.