1. Closed Circuit Television (CCTV) Policy & Guidance

1.1 Statement of Intent

Gulf English School Kuwait is committed to maintaining a safe and secure environment for all students, staff, visitors, and parents. To this end, we use closed-circuit television (CCTV) surveillance systems to monitor and record activities within school premises. This policy establishes the framework for the lawful, fair, and transparent use of CCTV systems in compliance with:

- Kuwait Law No. 61 of 2015 (Privacy and Data Protection)
- Ministry of Interior regulations on surveillance systems
- Ministry of Education 2018 circular on cameras in private schools
- Local school governance and safeguarding requirements
- Best practices in school safety and security management

The purposes of this policy are to:

- Ensure CCTV systems are used lawfully and ethically
- Protect the rights and privacy of data subjects
- Establish clear guidelines for access, retention, and disclosure of footage
- Provide transparency to the school community regarding surveillance activities
- Maintain recorded evidence for investigation and safeguarding purposes

---

1.2 Definitions

For the purposes of this policy:

CCTV (Closed Circuit Television): A system of video cameras and recording equipment that captures moving and still images of individuals and/or areas for security and safeguarding purposes.

Overt Surveillance: The visible use of surveillance cameras with clear signage and notification that recording is taking place. Individuals are aware they may be recorded.

Covert Surveillance: The hidden use of surveillance cameras without the knowledge of those being recorded. Gulf English School does not employ covert surveillance.

Data Subject: Any individual whose image or personal information is captured by CCTV systems.

Data Controller: The senior member of school management responsible for ensuring CCTV is used lawfully and in accordance with applicable legislation (Security Supervisor).

Data Protection Lead (IT Manager): The designated staff member responsible for overseeing data protection compliance, including CCTV governance.

Footage Retention Period: The length of time surveillance recordings are stored before automatic deletion. Standard retention: 120 days for routine footage; extended retention only for ongoing investigations or legal proceedings.

Access Request: A formal request from a data subject or authorized party to view or receive copies of CCTV footage containing their image.

1.3 Roles and Responsibilities

Data Protection Lead (IT Manager)

The Data Protection Lead holds the following responsibilities:

- Overseeing all CCTV operations and ensuring compliance with Kuwait Law 61/2015 and school policy
- Processing and responding to access requests from data subjects (students, parents, staff)
- Approving the retention of footage beyond standard periods for investigations or legal purposes
- Ensuring that all CCTV footage containing personal data is securely stored and protected from unauthorized access
- Maintaining comprehensive records of camera locations, footage access logs, exports, data subject requests, and system maintenance
- Reviewing CCTV policy annually and providing staff training
- Conducting quarterly compliance audits

Data Controller (School Director/Principal)

The School Director acts as the Data Controller with overall responsibility for:

- Approving camera installations and ensuring lawful purposes
- Determining staff access levels and overseeing operations
- Authorizing disclosures to third parties and ensuring signage compliance

Data Controller (School Director/Principal)

The School Director acts as the Data Controller with overall responsibility for:

- Approving camera installations and ensuring lawful purposes
- Determining staff access levels and overseeing operations
- Authorizing disclosures to third parties and ensuring signage compliance

Security Team & Authorized Staff

Authorized staff must only access footage for approved purposes, maintain confidentiality, document all access, and report issues immediately.

1.4 Purposes and Justification

CCTV systems at Gulf English School Kuwait serve these specific purposes:

- **Protecting school property and assets** (deterring crime/vandalism)
- **Promoting the health and safety of staff, pupils, and visitors** (safeguarding)

- **Assisting law enforcement in deterring and detecting crime**
- **Student and Staff Safety:** Preventing violence, bullying, harassment
- **Property Protection:** Documenting theft, vandalism, unauthorized entry
- **Security Management:** Monitoring access points and emergencies
- **Evidence Collection:** Supporting internal and external investigations

Proportionality Assessment: The surveillance must be necessary and proportionate to the identified purpose. Camera placement is justified only where no less intrusive alternative exists, and coverage is limited to what's required.

1.5 CCTV Camera Locations and Coverage

There are 203 CCTV cameras at GES covering:

- Main entrance gates and vehicle access points
- Reception area and lobby
- School corridors and hallways

- Stairways and emergency exits
- Playground and outdoor recreational areas
- Parking areas (staff and visitor)
- Perimeter of school grounds
- Administrative offices (common areas only)
- Cafeteria and common areas

1.5 Restriction on Placement

CCTV recording is strictly prohibited in areas where individuals have a heightened expectation of privacy. This includes, but is not limited to:

- Toilets and bathroom facilities
- Changing rooms and locker rooms
- Individual staff offices
- Staff break rooms
- Dedicated prayer rooms
- First-aid rooms
- Counselling areas
- Medical/nurse office (clinical areas)
- Private assessment rooms

1.6 Procedures Summary

CCTV Control Room/Server Area Security:

- Access is **strictly limited** to named, authorized staff members approved by the School Director
- **Non-authorised personnel** (general staff, students, visitors) are **strictly prohibited**
- External parties (contractors, law enforcement, auditors) require **continuous supervision** by authorized IT staff
- **All entrants must sign the Access Log Book** recording: Name, Date, Time & Specific Purpose
- **Personal mobile phones, cameras, or recording devices are strictly not allowed** in the Control Room
- **Downloading/copying footage prohibited** unless following documented Disclosure Procedure

- All media used (USB drives) must be **fully encrypted, password-protected,** and returned to IT
- **Live/recorded footage accessed only for legitimate purposes** (safety, crime prevention, investigations) – never for curiosity
- **Security staff present** at all times footage is reviewed by authorized personnel

Retention: Maximum 120 days; automatically overwritten/deleted unless flagged for investigation. All exceptions logged and reviewed by the IT Manager.

Technical Audits: Designated IT staff conduct documented checks confirming:

- All cameras recording properly
- DVR/NVR hardware functioning
- Time/date stamps are accurate and synchronized

1.7 Data Protection Principles

CCTV processing follows these principles:

- **Lawful Basis:** Legitimate interests in safety and property protection (Kuwait Law 61/2015)
- **Fairness/Transparency:** Clear signage at all entry points
- **Purpose Limitation:** Security use only; no repurposing
- **Data Minimization:** Automatic deletion after 120 days
- **Security:** Isolated network, encrypted storage, no remote access
- **Accountability:** Full audit logs and annual reviews

1.8 Retention Schedule

- **Standard:** 120 days (automatic overwrite) 24/7 recording. (if set to motion detection the recording time will reset to 180+ days
- **Extended:** Only for active investigations/legal proceedings, max 6 months, IT Manager-approved and logged (IT needs to be informed in advance)

1.9 Access to CCTV Footage

Authorized Personnel Only:

- School Director, Head of Security, IT Manager, Deputy Director, SLT

- CCTV footage is not shown to or shared with parents
- The school will provide CCTV footage upon request to official external authorities (e.g. the Police, Ministry of Education)

Mandatory Access Logging:
| Date | Time | Accessed By | Camera/Area | Purpose | Duration | Copied

---

1.10 Data Subject Rights & Disclosure

- **Access Requests:** Processed within 5 days if feasible; in-person viewing preferred
- **Parents:** Specific incident footage only, no general copies
- **Law Enforcement:** Provided with warrant; documented without
- **Refusals:** Explained in writing with appeal rights

1.11 Training & Review

- **Training:** Annual for authorized staff
- **Audits:** Weekly technical, quarterly access log reviews
- **Policy Review:** Annual by IT Manager/Director

1.12 Breach & Disciplinary Action

Unauthorized access results in warnings, access suspension, termination, or law enforcement referral

---

Policy Author/IT Manager: Douglas Pereira, IT Manager, dpereira@tes.com.kw
Approved by: [Director Name] **Date:** [Date] **Review:** [Date +12 months]