



AMBASSADOR

Education Group



CCTV Policy & Procedures

AEG EHS Department

2024/2025



TABLE OF CONTENTS





AEG CCTV Policy and Procedures

1. Mission, Vision & Values

Mission: To produce well-rounded, academically successful, happy young men and women.

Vision: To engage, inspire and extend our students, our staff, and the wider community.

Values: To create a community where everyone mirrors our values of good manners, kindness, and wisdom.

2. Purpose

AEG schools are committed to ensuring the safety and security of their students, staff, and visitors while protecting personal data under the Personal Data Protection Act B.E. 2562 of Thailand. This policy establishes clear guidelines for the installation, operation, and management of closed-circuit television (CCTV) systems within the AEG schools, ensuring compliance with Thai PDPA laws and international best practices.

3. Scope

This policy and procedures apply to all CCTV systems operated by the AEG schools, including cameras installed on campus, at entry/exit points, hallways, common areas, and outdoor spaces. It covers the collection, storage, access, processing, and disclosure of recorded footage. CCTV systems will not be used to monitor normal teacher/student classroom activity.

4. Legal Basis & Compliance with Thai PDPA

The AEG schools acknowledge their duty to comply with Thai PDPA and other relevant laws. The CCTV system is operated based on the legitimate interests of safeguarding the schools community, preventing crime, and managing security incidents. The AEG schools ensure that CCTV systems are used responsibly and safeguard both trust and confidence in its continued use.



5. CCTV Management & Operation

- The AEG CAA is responsible for the governance of CCTV operations.
- The AEG EHS Director oversees compliance with Thai PDPA regulations.
- The AEG IT Department ensures secure technical operation and maintenance.
- The IT Team of each school is responsible for CCTV system operation and monitoring, under the oversight of the school's leadership team.
- All authorized personnel with access to CCTV images are trained in their responsibilities and must follow proper procedures.
- CCTV is not monitored centrally by AEG or its schools administration.
- The CCTV system is owned and operated by AEG and its schools, with deployment decisions made by each school's Leadership Team.
- CCTV surveillance at the School is intended for:
 - Protecting school buildings and assets.
 - Ensuring the health and safety of staff, students, and visitors.
 - Preventing bullying and antisocial behavior.
 - Assisting police and security teams in crime deterrence and detection.
 - Identifying and prosecuting offenders.
 - Ensuring adherence to school rules.

6. Responsibilities

Each Head of AEG school supported by AEG IT department (or nominated person) will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by AEG;
- Oversee and coordinate the use of CCTV monitoring for safety and security purposes within AEG schools;
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy;
- Ensure that the CCTV monitoring at school is consistent with the highest standards and protections;
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy;



- Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system;
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally;
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment;
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place;
- Cooperate with the IT Department in reporting on the CCTV system in operation in the school;
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of “Reasonable Expectation of Privacy”;
- Ensure that monitoring footage are stored in a secure place with access by authorised personnel only;
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 30 days and are then erased unless required as part of an investigation or court proceedings (criminal or civil);
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy;
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics;
- Ensure that camera control is not infringing an individual’s reasonable expectation of privacy in public areas.



7. CCTV System Usage

- CCTV cameras shall be positioned to avoid unnecessary intrusion into private spaces (e.g., restrooms, staff offices and rooms).
- Video surveillance shall be conducted only for security, safety, and incident investigation purposes.
- AEG schools shall not use CCTV for monitoring employee performance or student behavior unless related to security concerns.
- CCTV footage shall not be used for personal, commercial, or unauthorized purposes.
- CCTV monitoring of public areas shall be conducted in a manner consistent with school policies.
- Covert surveillance is **strictly prohibited**.

8. Data Collection, Storage & Retention

- Recorded footage is stored securely in a controlled environment with restricted access.
- Footage is retained for a maximum of **30 days**, unless required for an ongoing investigation or legal proceedings.
- If footage captures criminal activity or health and safety risks, it may be retained longer for investigative purposes.
- After the retention period, footage is permanently deleted in a secure manner.

9. Subject Access Requests (SAR)

- Access to CCTV footage is limited to authorized personnel.
- Individuals have the right to request access to CCTV footage relating to themselves under the Personal Data Protection Act.
- Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.
- The school will respond to requests within 15 calendar days of receiving the request in line with the school's right of access policy.
- The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.
- A record of the date of the disclosure along with details of who the information has been provided to (the name of the person and the organisation they represent) and why they required it, will be made.



- In giving a person a copy of their data, the school provides a still or series of still pictures, a tape or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.
- Where footage contains images relating to the third parties, the school will take appropriate steps to mask and protect the identities of those individuals.
- CCTV footage may be shared with law enforcement agencies only when legally required or to assist in security-related investigations.
- Access to recorded footage will always require the presence of **two authorized staff members**, and a written access log will be maintained (*see Appendix 1.*)
- In cases where a recording contains sensitive material, access will be determined by the **Head of School**.

10. Location of Cameras

- Cameras will be placed strategically to capture images relevant to security purposes while respecting privacy rights.
- Outdoor cameras shall be positioned to **minimize recording of passers-by or private properties**.
- CCTV will **not** monitor areas where individuals have a reasonable expectation of privacy.
- Video monitoring and recording may cover:
 - **Classrooms, Canteens and Gymnasiums.**
 - **Perimeter security**, including fences, gates, and roads.
 - **Entrances/exits, lobbies, and hallways.**
 - **Storage areas and office locations.**
 - **Access control points and alarm systems.**
 - **Child protection and criminal investigations** in collaboration with law enforcement.

11. Complaints

- Complaints regarding CCTV operation should be directed to the **AEG CAA** in the first instance.



12. Staff Training

- Staff authorized to access the CCTV system will receive **training** on handling and securing surveillance data.
- Training will include procedures for responding to disclosure requests and regulatory compliance.
- **Misuse of CCTV footage** will result in disciplinary action.

13. Policy Review & Updates

- This policy shall be **reviewed annually** or as required by changes in regulations.
- Next scheduled review: **August 2025**.
- Any updates shall be communicated to stakeholders accordingly.

14. Contact Information

For any inquiries regarding this policy, please contact:

Data Protection Officer (DPO)

Ambassador Education Group AEG,
229/20 Moo 2 Tambol Nong-Phueng
Amphur Sarapee, Chiang Mai 50140
www.aegcm.com / info@aegcm.com

This policy is designed to align with the Thai Personal Data Protection Act B.E. 2562 (PDPA) and international best practices for data privacy and security.