



TCIS CCTV Policy

1. Purpose

This CCTV Usage Policy establishes the guidelines for the use of closed-circuit television (CCTV) within the Thai- Chinese International School (referred to as “TCIS” in this policy) located 101/177 Moo 7 Soi Mooban Bangpleenives, Prasertsin Road, Bangplee Yai, Samutprakarn 10540 Thailand.

The CCTV equipment is in use for the following purpose:

- Prevention, investigation, and detection of crimes against person and/or property
- Apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings)
- Safety of students, visitors, contractors, employees, and staff
- Monitoring the security of premises and assets

2. Scope

This CCTV Policy applies to all areas controlled by TCIS.

This CCTV Policy applies to all TCIS students, employees, staff, contractors, and visitors.

This CCTV Policy is guided by and supports the relevant requirements of the

Thailand Personal Data Protection Act, B.E.2562 (“PDPA”).

All CCTV footage disclosure must be approved by the Data Protection Officer and the IT Director.

3. Siting Usage of cameras and Signate

CCTV data shall not be used for purposes other than as stated above. CCTV cameras are installed and positioned such that they will only monitor those strategic points or spaces which are intended to be covered, except certain areas such as changing rooms, toilets, and shower rooms. Warning signs, as required by the legislation, are placed within the campus areas covered by the CCTV cameras. The cameras shall be limited/restricted in their movement so that they cannot be manipulated beyond their intended coverage zones. CCTV operators shall be aware of the privacy implications of CCTV usage.

4. Records Storage and Retention

- Generally, data shall be retained for a period of 28 days, after which it must be deleted in lines with the principle of data limitation. TCIS can define a longer period if this can be justified.
- Specifically, if data is in use for investigation or evidential purposes then the data shall be retained for as long as required by the investigation.
- If the data is retained for evidential purposes, it shall be retained in a secure place to which access is controlled.
- Monitors displaying images from areas in which individuals have an expectation of privacy shall not be viewed by anyone other than authorized operators of the equipment.
- Access to and viewing of the recorded images is restricted to the IT Director or designated member of staff, who will decide whether to allow requests for access by third parties in accordance with our documented disclosure procedure.
- The removal and return of media for viewing purposes shall be documented.
- All operators and employees with access to images shall be aware of the procedure for accessing the images.

- The removal and return of media for use in legal proceedings shall be documented.
- All relevant employees or CCTV equipment operators shall be familiar with and shall follow our policies and procedures on records retention and storage.

5. Access by, and disclosure of images to third parties

- Access to recorded images is restricted to accredited employees.
- All access to storage media shall be documented.
- Disclosures shall be governed by a disclosure agreement unless such disclosure is required by law.
- All requests for access or for disclosure shall be documented. If access or disclosure is denied, then the reason shall be documented.
- Disclosure to third parties is limited to the following circumstances:
 - Law enforcement agencies where the images recorded would assist in a specific criminal enquiry
 - Prosecution agencies
 - Relevant legal representatives
 - People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)
 - No disclosures shall be made to the media unless under direction of our communications policy and in accordance with the requirements of the relevant agency
 - Images are NOT to be made widely available - such as on the Internet

6. Data subject access

All relevant employees or CCTV equipment operators must be able to recognize a request for access and shall be familiar with and follow our data subject access request procedure.

7. Data subject rights

Subject to the conditions and exceptions under the applicable laws, you may have the rights to access and/or obtain a copy of, port, rectify, delete, destroy, or anonymize certain CCTV data that TCIS have about you, restrict and/or object to certain activities, in which TCIS engage with respect to your personal data. If your personal data is processed on your consent, you may withdraw your consent, but TCIS may not be able to provide you with its goods or services. You may also have the right to request TCIS to disclose how your personal data is obtained without your consent and lodge a complaint with the competent authority under the applicable laws.

8. Contact

If you have questions or concerns or would like to exercise your rights in relation to your CCTV data, please contact us or our Data Protection Officer at:

Thai- Chinese International School

101/177 Moo 7 Soi Mooban Bangpleenives,
Prasertsin Road, Bangplee Yai,
Samutprakarn 10540 Thailand.

Tel: 0-2751-1201

Email: dpo@tcis.ac.th

9. Review

This CCTV Policy is dated 24/05/2022 and will be reviewed by TCIS annually or upon development of the concerning technology to ensure effective and appropriate security measures, and in line with minimum legal requirement as prescribed by the laws relevant authorities.