Data Protection Policy

Updated July 2025

Centurion International School, Bangkok

CISB Data Protection Policy - 2025-2026

Purpose

Centurion International School of Bangkok (CISB) is committed to protecting personal data of students, parents, staff, contractors and other individuals in accordance with applicable Thai data protection laws, international school accreditation standards, and international school best practices. This Policy sets out how CISB collects, uses, stores, discloses and disposes of personal data, and how data subjects can exercise their rights.

Scope

This Policy applies to all personal data in the School's possession or control, whether electronic or paper-based, and covers:

1. All employees, contractors, volunteers and third-party service providers;
2. All School departments and activities, including academic, administrative, extracurricular, human resources and communications;
3. Personal data relating to students, parents/guardians, staff, alumni, visitors and any other individuals whose data the School processes.

Definitions

1. Personal data: Any information relating to an identified or identifiable natural person
2. Processing: Any operation performed on personal data (e.g., collection, use, storage, disclosure, erasure)
3. Data subject: The individual whose personal data is processed
4. Controller: The School, which determines the purposes and means of processing
5. Processor: A third party that processes personal data on behalf of the School
6. Data Protection Officer (DPO): The person or team designated by the School to oversee PDPA compliance

Data Protection Principles

In all data processing activities, the School will ensure that personal data is:

1. Lawfully, fairly and transparently processed;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
3. Limited to what is necessary in relation to the purposes for which it is processed;
4. Accurate and kept up to date;
5. Retained (in identifiable form) only as long as necessary;

6. Processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

Lawful Basis for Processing

The School will only process personal data where it has a valid legal basis, such as:

1. Consent of the data subject (or parent/guardian for minors);
2. Performance of a contract (e.g., enrollment agreement);
3. Compliance with legal obligations;
4. Vital interests (e.g., medical emergencies);
5. Public interest or legitimate interests of the School (e.g., safeguarding and school administration), provided these do not override the rights of data subjects.

Collection, Use and Disclosure of Personal Data

1. The School collects only data necessary for educational, administrative, health and safety and related purposes
2. Personal data is obtained directly from data subjects or their lawful representatives wherever possible
3. The School will not sell, rent or otherwise disclose personal data to third parties except:
    a. With the data subject's consent;
    b. To other education providers, government authorities or law enforcement as required by law;
    c. To service providers under contract subject to strict confidentiality and security obligations.

Data Security

Appropriate technical and organizational measures are in place to protect personal data, including:

1. Access controls (unique login credentials; role-based permissions)
2. Secure backup and recovery procedures
3. Regular security patching, vulnerability testing and audits
4. Secure disposal of physical records (shredding) and electronic media

Data Breach Response

1. Any actual or suspected personal data breach must be reported immediately to the DPO
2. The DPO will investigate, contain and remediate the breach, document its causes, and notify the affected data subjects if required by law
3. Lessons learned will be incorporated into policies and controls to prevent recurrence

Roles and Responsibilities

1. **Head of School**
    a. Ultimate authority for data protection, including CCTV policy decisions

b. Serves as Data Protection Officer (DPO)
c. Ensures adequate resourcing for data protection compliance
d. Advises on The Personal Data Protection Act 2012 (PDPA) obligations, monitors compliance and serves as point of contact for data subjects and regulators

2. **ICT Department**
    a. Implements and maintains technical security measures

3. **All Staff**
    a. Must follow this Policy
    b. Must complete required training, report breaches and handle personal data only as authorized

CCTV Footage Policy

1. **Purpose**
   CCTV cameras are installed on campus primarily to:
    a. Enhance the safety and security of students, staff and property;
    b. Support incident investigations and compliance with legal obligations (e.g., safety regulations).

2. **Coverage**
    a. Cameras are placed in public areas (entrances, hallways, common areas, perimeter)
    b. No CCTV cameras are installed inside private areas such as restrooms or changing rooms

3. **Access**
    a. Access to live feeds and stored footage is strictly limited to the Head of School, Head of Admin, the Dean of Students, and the on-site Board Representative

4. **Prohibition on Sharing with Families/Parents**
   Due to child protection purposes, and in alignment with international standards, under *no circumstances* will CCTV footage from classrooms or any other campus location be shared with families or parents, whether for viewing, copying or distribution. This prohibition applies even if families/parents request footage of their own children.

5. **Exceptions**
   Footage may only be disclosed to:
    a. Law enforcement or government authorities upon lawful request;
    b. The Head of School, for the purpose of internal investigations, disciplinary proceedings or safeguarding incidents.
    c. The Head of School is the ultimate decision-maker regarding any disclosure of CCTV footage. All requests for release or viewing of footage must be submitted in writing to the Head of School, who may delegate review but holds final sign-off authority.

7. Training and Awareness

a. All employees must complete data protection training upon hire and annual refresher courses
b. Specialized training for staff handling sensitive data (e.g., finance, HR, health records, security)

8. Third-Party Processors

a. All contracts with external vendors who process personal data on the School's behalf must include data protection clauses reflecting this Policy and PDPA requirements
b. The Head of School/DPO will conduct due diligence and periodic audits of processors

9. Monitoring and Review

a. This Policy will be reviewed at least annually or whenever there is a significant change in law, regulation or School operations
b. Updates will be approved by the Head of School and circulated to all staff

10. Enforcement

a. Non-compliance with this Policy may result in disciplinary action, up to and including termination of employment or contract, and may carry legal penalties under the PDPA

Date of Last Review: July 2025
Next Review: July 2026