CCTV POLICY

1. PURPOSE

1.1 The purpose of this Policy is to govern the installation and use of Closed-Circuit Television (CCTV) systems at Indie Education.

1.2 The primary objectives are to:

(a) Enhance the safety and security of students, employees, and visitors.

(b) Protect school property against theft, vandalism, and damage.

(c) Deter inappropriate behaviour and ensure a safe educational environment.

(d) Assist in the investigation of incidents and the identification of individuals involved in security breaches.

(e) Provide evidence for disciplinary actions and law enforcement.

2. SCOPE

2.1 This Policy applies to all CCTV systems installed on Indie Education premises, including but not limited to classrooms, hallways, playgrounds, parking areas, and other public spaces within the school grounds.

3. ACCOUNTABILITY

3.1 Key responsibilities under the policy:

(a) Head of ICT | ICT Team Leader:

i. Acts as the site owner(s) for all CCTV Systems.

ii. Seek approval from Finance and/or the Executive team for procurement and installation.

iii. Provide video footage to approved persons as requested.

iv. Review site requirements.

v. Authorise review and audit activities.

(b) Executive Manager | Executive Principal:

i. Authorise CCTV site setup.

ii. Request audit of CCTV systems.

iii. Request footage to be provided to company employees or law enforcement.

iv. Request changes to this policy.

(c) CEO and Deputy CEO:

i. Review CCTV requirements.

ii. Authorise CCTV footage and investigation.

4. COMPLIANCE

4.1 The installation and use of CCTV systems must comply with the following legislation and guidelines:

(a) Privacy Act 1988 (Cth),

(b) Surveillance Devices Act 2007 (NSW) or equivalent state legislation,

(c) Australian Privacy Principles (APPs), and

(d) Relevant state education department policies and guidelines.

5. INSTALLATION AND PLACEMENT

5.1 Approval and Consultation

(a) CCTV installation must be approved by the Head of ICT and the Executive Team.

(b) Consultation with employees, students, and parents (if required) should be conducted prior to installation to address any concerns and ensure transparency.

5.2 Placement of Cameras

(a) Cameras must be positioned in areas that are deemed necessary for security purposes, preference is given to entry points.

(b) Cameras should not be installed in private areas such as classrooms, bathrooms, changing rooms, common areas, or employee areas.

(c) Signage must be prominently displayed to inform individuals that CCTV is in operation.

(d) ICT will work with the site manager to determine the camera placement.

(e) ICT will generate a camera layout diagram to record camera locations for the site.

5.3 Installation of CCTV System

(a) Installation can only be carried out by an approved and licenced contractor or company employee. Contractors must be able to provide evidence of accreditation before commencement.

(b) All CCTV system account details must be provided to the Head of ICT within 10 working days.

(c) ICT will configure all CCTV equipment before deliver to the allocated site.

6. USE OF CCTV FOOTAGE

6.1 Monitoring

(a) CCTV footage should be monitored by authorised employees only, such as the site manager, designated ICT employees, or the Company executive team.

(b) Live monitoring should be limited to times when security concerns are heightened.

6.2 Access to footage

(a) Access to recorded footage is restricted to authorised employees only.

(b) Requests for access to footage by external parties (e.g., law enforcement, parents) must be formally submitted and approved by the Head of ICT.

(c) No access will be granted to contractors.

(d) CCTV footage may be used for investigating security incidents, disciplinary actions, or legal proceedings.

(e) Footage should not be used for monitoring employee performance or student behaviour unless related to a security incident.

7. STORAGE AND RETENTION

7.1 Storage

(a) CCTV footage must be stored securely to prevent unauthorised access, alteration, or deletion.

(b) Footage should be stored in encrypted formats where possible.

7.2 Retention period

(a) CCTV footage should be retained for a minimum of 30 days and a maximum of 90 days, unless required for an ongoing investigation.

(b) After the retention period, footage should be securely deleted or overwritten.

8. PRIVACY AND CONFIDENTIALITY

8.1 The use of CCTV systems must respect the privacy rights of individuals in accordance with the Privacy Act 1988.

8.2 Personal information captured by CCTV must be handled in a manner consistent with the Australian Privacy Principles.

9. ACCOUNTABILITY AND REVIEW

9.1 **Accountability**

(a) The Company executive team are responsible for ensuring compliance with this policy.

(b) The Head of ICT is appointed as the CCTV system administrator to manage day-to-day operations.

9.2 **Review**

(a) This policy should be reviewed annually to ensure its effectiveness and compliance with any changes in legislation or Company requirements.

(b) Feedback from employees, students, and parents should be considered during the review process.

10. BREACH OF POLICY

10.1 Any breach of this policy may result in disciplinary action in accordance with the company's code of conduct.

10.2 Serious breaches may be reported to the relevant authorities for further investigation.

11. POLICY REVIEW

11.1 In accordance with Indie Education's policy review protocol, this Policy will be reviewed annually. If there are material changes to circumstances before the 12-month period, this Policy will be reviewed immediately to ensure its contents remain effective and up to date.

12. AUTHORISATION

12.1 This Policy has been reviewed and approved in accordance with the delegations set out in the Chief Executive Officer Limitations Policy and is available to the Board and the Chief Executive Officer for ongoing consideration.