1.26 CLOSED-CIRCUIT TELEVISION (CCTV) POLICY

1. Rationale

Mandalika Intercultural School (MIS) operates a closed-circuit television (CCTV) system as part of its safeguarding, safety and security arrangements. Because CCTV images may identify individuals and may include children, access must be strictly limited, purposeful, confidential and accountable.

2. Purpose:

This policy establishes how MIS uses CCTV to help provide a safe and secure environment for students, staff and visitors while respecting privacy and preventing inappropriate access, use or disclosure.

3. Scope:

This policy applies to all CCTV systems operated by or on behalf of MIS and to all students, staff, Board Members, visitors, contractors and service providers on MIS premises.

4. Objectives:

- To deter and detect unauthorized access, theft, vandalism, and other security breaches.
- Support safeguarding, health and safety, and the investigation of incidents or complaints.
- Provide relevant evidence for authorised internal investigations or lawful external requests.
- Protect school premises, people and assets while using CCTV proportionately.

4. Camera Locations and Privacy:

Cameras may be installed at entrances and exits, hallways and corridors, the library and sickbay, playgrounds and outdoor areas, administrative areas, and other locations supported by a documented safety or security need.

● Cameras must not be installed in toilets, changing areas or any location where a person would reasonably expect privacy.

● Camera positioning must avoid unnecessary viewing of neighbouring properties or public areas.

● The Head of School must periodically review camera locations to confirm that each remains necessary and proportionate

6. Permitted Use

Live or recorded CCTV may be accessed where reasonably necessary for safeguarding, school safety, security, access control, parking and traffic management, supervision of school premises, operational oversight, incident response, system testing, an authorised investigation or a lawful request.

The School Board, Director and Head of School may use CCTV to observe the general operation of the School and identify safety, security, traffic, supervision or operational issues. Such monitoring must be proportionate and connected to a legitimate School purpose.

CCTV must not be used for personal purposes, general curiosity, or continuous targeted monitoring of an individual employee or student without a documented safeguarding, safety, security, misconduct or other legitimate operational reason. CCTV footage may be considered when investigating a specific incident or concern involving staff or students.

7. Access Restrictions

Routine system access is restricted to:

● the School Board, acting through the Board Chair or another Board member specifically authorised by the Board;

● the Director(s) ; and

● the Head of School.

No other employee, contractor, parent, student or visitor may receive login credentials or independent access to live feeds, recorded footage, playback, export or administration functions.

Where operationally necessary, a person outside the authorised access group may be shown a limited and relevant extract, but only under the direct supervision of an authorised person and only when required for a legitimate purpose. This does not grant system access. Technical personnel may perform maintenance without viewing footage wherever possible; any necessary viewing must be authorised, limited and logged.

Access credentials are individual and confidential. Shared accounts and password sharing are prohibited. Access rights must be removed promptly when a person changes role or leaves MIS.

8. Requests, Approval and Emergency Access

- Requests to view or obtain footage must be made in writing to the Head of School and must state the date, approximate time, location, persons or incident involved, and reason for the request.

- The Head of School will approve or deny the request, consult the Director where the matter is sensitive or contested, and refer requests involving the Head of School to the Director. Requests involving the Director must be referred to the Board Chair.

- In an urgent safeguarding, health or security emergency, the Head of School, Director or authorised Board representative may permit immediate access. The reason, persons involved and action taken must be entered in the access register as soon as practicable.

- Only the minimum footage necessary for the approved purpose may be viewed or exported.

9. Head of School Responsibilities

The Head of School is responsible for managing implementation of these access restrictions and must:

- maintain the current list of authorised users and ensure permissions reflect this policy;

- maintain a CCTV Access Register recording each viewing, search, export, disclosure or exceptional technical access, including the requester, authoriser, purpose, date/time and footage concerned;

- ensure credentials, monitors, exported files and storage equipment are appropriately secured;

- ensure relevant personnel understand confidentiality and access requirements;

- coordinate preservation of footage connected with an incident, complaint, investigation or legal request;

- report suspected unauthorised access, loss, copying or disclosure promptly to the Director(s) and Board Chair; and

- review access permissions and the Access Register at least once each school term.

10. Storage, Retention and Security

- Footage will be stored securely on an MIS-controlled recorder, server or approved system, protected by appropriate physical and technical safeguards.

- Routine footage will normally be retained for no longer than 30 days and then automatically overwritten or securely deleted.

- Footage required for an incident, complaint, investigation, insurance matter or legal request may be preserved for as long as reasonably necessary for that purpose. The reason and disposal date must be recorded.

- Exports must be limited, encrypted or password-protected where practicable, and stored only in an authorised location. Uncontrolled copying to personal devices, personal email, messaging applications or personal cloud storage is prohibited

11. Disclosure and Confidentiality

CCTV images and information derived from them are confidential. Footage may be disclosed outside MIS only when authorised by the Head of School together with the Director(s) (or by the Board Chair where either is involved), and only where there is a legitimate safeguarding, legal, regulatory, insurance or law-enforcement reason. The disclosure must be recorded. Where practicable, unrelated persons should be obscured or the recipient should view footage under supervision rather than receive a copy.

12. Notification

- Clear signage will be displayed at entrances and other appropriate locations to notify individuals that CCTV is in use.

- This policy will be communicated through appropriate school channels and made available on request.

13. Breach of Policy

Unauthorised access, viewing, recording, copying, sharing, alteration or deletion of CCTV footage may result in disciplinary action, withdrawal of access, termination of contract, referral to relevant authorities, or other action appropriate to the circumstances.

14. Review

The Head of School will review implementation annually and recommend changes to the School Board. The School Board retains responsibility for approving this policy and material amendments

Version	Approved by:	Date of issue:
2	School Board	7th August 2026