AUSTRALIAN
ISLAMIC COLLEGE

EST. 1986

CCTV & CAMERA ACCESS MANAGEMENT POLICY & PROCEDURE

Postal Address PO Box 252, Cloverdale, WA 6985
Ph 08 9362 2100 **Email** info@aic.wa.edu.au **Website** www.aic.wa.edu.au

Thornlie College 17 Tonbridge Way, Thornlie, WA 6107 **Ph** 08 9493 2718
Dianella College 81 Cleveland St, Dianella, WA 6108 **Ph** 08 9375 9770
Kewdale College 139 President Street, Kewdale, WA 6105 **Ph** 08 9362 2100
Henley Brook College 10 Asturian Drive, Henley Brook, WA 6055 **Ph** 08 9375 9892
Forrestdale College 651 Nicholson Road, Forrestdale, WA 6112 **Ph** 08 9493 5819
Adelaide College 22A Cedar Avenue, West Croydon, SA 5008 **Ph** 08 8340 7799

Table of Contents

1. Purpose & Scope

This policy outlines the guidelines for the installation, management, operation, and access control of the Closed-Circuit Television (CCTV) systems across all Australian Islamic College (AIC) campuses. It ensures a safe and secure environment for students, staff, and visitors, and establishes proper surveillance management practices in line with Australian privacy and cyber laws.

This policy applies to:

- The installation and operation of CCTV systems.
- The management, access, use, and disclosure of surveillance footage.
- All AIC staff, students, visitors, and authorised external parties.

2. Legal & Compliance Framework

AIC adheres to the following Australian laws and regulations:

- **Privacy Act 1988 (Cth)** – Governs the handling of personal information and surveillance data.
- **Australian Privacy Principles (APPs)** – Outlines obligations for handling personal information.
- **Surveillance Devices Act 2004 (Cth)** – Regulates the use and disclosure of surveillance recordings.
- **Surveillance Devices Act 1988 (WA)** / **Surveillance Devices Act 2016 (SA)** – Governs state-specific surveillance protocols.
- **Security of Critical Infrastructure Act 2018** – Protects critical digital and physical infrastructure.
- **Other relevant AIC policies**, including:
  - Privacy Policy
  - Risk Management Policy
  - Network Security Policy
  - Records Management Policy
  - Transportation Policy

3. Roles & Responsibilities

3.1 Approving Authorities

- Executive Principal / CEO
- Business Manager
- Principal

The “approving authorities” are responsible for all access approvals to the CCTV system and surveillance footage.

3.2 ICT Officers

- Responsible for managing system access, maintaining security protocols, and ensuring compliance.
- Grant or revoke camera access based on written approval from an authorised authority.

3.3 Authorised Users

Access is granted strictly on a **role-based, need-to-know basis** to:

- Executive Principal / CEO
- Business Manager
- Principal
- Chief Information Officer (CIO)
- ICT Officers

External third parties (e.g. law enforcement) may only access footage with written approval and a signed Non-Disclosure Agreement (NDA).

4. Access Control Measures

4.1 Role-Based Access (RBAC)

- **ICT Officers**: Full access (configuration, monitoring, and footage retrieval).
- **Authorised personnel**: View-only access, where necessary.

4.2 Authentication & Security

- Multi-Factor Authentication (MFA) is mandatory.
- No shared accounts; unique credentials for each user.
- Passwords must:
  - Be at least 12 characters long
  - Be changed every 90 days

4.3 Access Revocation

- Immediate revocation upon role change or termination.
- Annual access audits and compliance reviews.

5. Camera Operation & Locations

5.1 Purpose of CCTV Surveillance

CCTV is used to:

- Prevent and verify incidents involving criminal behavior or misconduct.
- Assist in emergency management.
- Protect College property from theft and vandalism.
- Investigate injury, loss, or damage to individuals or assets.

5.2 Camera Locations

CCTV cameras are positioned in the following non-private, high-traffic areas:

- Entrances and exits
- Corridors and locker areas
- Learning spaces and admin areas
- Playgrounds and ovals
- IT labs and libraries
- Car parks and buses

Note: Cameras are **not installed** in private areas (toilets, changing rooms).
Signs are posted near each camera to inform individuals of CCTV use.

6. Monitoring, Logging & Auditing

- All access logs are retained and reviewed periodically.
- Unauthorised access attempts must be immediately reported to ICT Officers.
- Quarterly security audits assess compliance and identify any risks or breaches.

7. Access to Footage

7.1 Internal Requests

- The principal may show incident-specific footage to involved staff, students, or parents **only** when relevant.
- Copies of footage **will not be distributed** to individuals.
- Requests must be submitted to the ICT Department.

7.2 Parent Requests

- If a parent challenges an incident and requests footage, the ICT Officer will generate a Helpdesk ticket.
- Approval must be received from **any** of the following:
  - Executive Principal/CEO

    - Business Manager
    - Principal
    - Chief Information Officer

7.3 Third-Party Requests

- Third party (e.g. police, legal counsel) requests must go through the IT Helpdesk system.
- NDA must be signed by:
    - The third-party requester
    - Approving authority
    - ICT Officer
- NDA must include penalties and compliance terms before footage is released.

8. System Management & Ownership

- The AIC IT Department is responsible for:
    - Operating and maintaining the CCTV system
    - Reviewing camera placements
    - Ensuring secure storage and handling of data
    - Upgrading equipment as required
- CCTV systems and all recorded footage are the **exclusive property of AIC**.

9. Storage & Retention of Footage

- Default retention: **7 days** unless footage is flagged for investigation.
- Extended retention for verified incidents or legal requirements.
- Secure storage protocols apply during the retention period.

10. Incident Response & Enforcement

- All unauthorised access must be reported within **24 hours** to the ICT Department.
- Policy breaches may lead to disciplinary actions, up to and including dismissal or legal consequences.
- Any breach involving personal data must be handled per the College's Privacy Policy and Data Breach Response process provided within that policy.

Last reviewed:	[May 2025]
Approved by:	[Executive Principal]
Next review:	[May 2026]