CLOSED-CIRCUIT TELEVISION (CCTV) AND VIDEO SURVEILLANCE POLICY

Ambition International School
Effective Date: 24 May, 2025
Review Date: 24 May, 2026
Version: 2.0

---

1. POLICY STATEMENT

Ambition International School is committed to providing a safe, secure learning environment for all students, staff, and visitors while respecting fundamental privacy rights and human dignity. This policy establishes clear guidelines for the ethical, legal, and proportionate use of CCTV surveillance systems on school premises.

Core Principles:

- **Safety First:** Protecting the welfare of our school community
- **Privacy Respect:** Minimizing intrusion while maintaining security
- **Transparency:** Clear communication about surveillance practices
- **Accountability:** Responsible use and access to recorded material
- **Compliance:** Adherence to all applicable laws and best practices

---

2. LEGAL FRAMEWORK AND COMPLIANCE

This policy operates within the framework of:

South African Legislation:

- Constitution of the Republic of South Africa, 1996 (Privacy rights - Section 14)
- Protection of Personal Information Act (POPIA), 2013
- South African Schools Act 84 of 1996 (SASA)
- Regulations for Safety Measures at Public Schools (Government Notice 1040/2001)
- Private Security Industry Regulation Act 56 of 2001

International Standards:

- UN Convention on the Rights of the Child
- Global Privacy Protection Guidelines
- International surveillance best practices

3. DEFINITIONS

Authorized Personnel: School officials designated by the Principal with specific authority to access, manage, or operate CCTV systems.

Data Subject: Any identifiable individual captured in CCTV footage.

Personal Information: As defined in POPIA - any information relating to an identifiable person.

Surveillance: The monitoring, observing, or recording of persons or activities through CCTV systems.

School Premises: All buildings, grounds, facilities, and areas under school control or management.

---

4. PURPOSE AND OBJECTIVES

4.1 Primary Purposes

- **Safety Protection:** Safeguarding students, staff, and visitors from harm
- **Crime Prevention:** Deterring theft, vandalism, and other criminal activities
- **Incident Investigation:** Providing evidence for disciplinary or legal proceedings
- **Emergency Response:** Supporting rapid response to medical or safety emergencies
- **Property Protection:** Securing school assets and infrastructure

4.2 Specific Objectives

- Maintain a violence and drug-free school environment
- Prevent bullying, harassment, and inappropriate behavior
- Monitor access points and perimeter security
- Support child protection and safeguarding obligations
- Enhance overall school safety culture

---

5. SYSTEM SPECIFICATIONS AND COVERAGE

5.1 Technical Infrastructure

- **Current System:** 10 strategically positioned HD cameras
- **Recording Quality:** Minimum 1080p resolution
- **Storage Capacity:** 30-day retention minimum (upgraded from 15 days)
- **Backup Systems:** Redundant storage with cloud backup capability

- **Access Controls:** Multi-factor authentication for all system access

5.2 Coverage Areas

Monitored Areas:

- Main entrance and reception areas
- Corridors and common areas
- Playgrounds and outdoor recreational spaces
- Parking areas and perimeter fencing
- Classrooms (audio recording prohibited)

Excluded Areas (Privacy Zones):

- Bathrooms and changing facilities
- Staff rest areas and private offices
- Counseling and medical rooms
- Areas where reasonable expectation of privacy exists

5.3 Camera Specifications

- Clearly visible and appropriately signposted
- Weather-resistant for outdoor installations
- Night vision capability for 24/7 monitoring
- Motion-activated recording with continuous backup
- Positioned to minimize viewing into neighboring private properties

---

6. PRIVACY PROTECTION MEASURES

6.1 Privacy by Design

- Cameras positioned to capture minimum necessary footage
- Privacy masking technology for sensitive areas
- Regular privacy impact assessments
- Staff training on privacy obligations

6.2 Data Minimization

- Recording only when necessary for stated purposes
- Automatic deletion after retention period
- Limited access on need-to-know basis
- Regular review of camera positioning and necessity

6.3 Individual Rights

Data subjects have the right to:

- Be informed about surveillance (through clear signage)
- Request access to footage containing their image
- Request correction of inaccurate records
- Lodge complaints about surveillance practices
- Understand how their personal information is processed

---

7. ACCESS AND DISCLOSURE PROTOCOLS

7.1 Authorized Access

Level 1 - Real-time Monitoring:

- Principal and designated Deputy Principal
- Head of Security (if appointed)
- Emergency response personnel during incidents

Level 2 - Recorded Footage Review:

- Principal or Deputy Principal
- Designated Child Protection Officer
- External investigators (with proper authorization)

7.2 Access Request Procedure

Written Application Required Including:

1. Full identification and contact details
2. Specific date, time, and location of requested footage
3. Detailed justification and legal basis for access
4. Intended use of the information
5. Confirmation of authority to request access

Review Process:

- All requests evaluated within 5 working days
- Consultation with legal counsel for complex requests
- Written response with detailed reasoning
- Appeals process available through School Governing Body

7.3 Third-Party Disclosure

Permitted Disclosures:

- Law enforcement agencies (with warrant or court order)
- Child protection services (statutory obligations)
- Legal proceedings (court-ordered disclosure)
- Insurance investigations (property damage claims)

- Emergency services (immediate safety concerns)

Prohibited Disclosures:

- Media or social media platforms
- Unauthorized third parties
- Commercial purposes
- Disciplinary proceedings at other institutions

---

8. DATA SECURITY AND RETENTION

8.1 Technical Safeguards

- Encrypted data transmission and storage
- Secure server infrastructure with restricted physical access
- Regular security updates and vulnerability assessments
- Backup systems with geographic separation
- Access logging and audit trails

8.2 Retention Schedule

Standard Retention: 30 days from recording date **Extended Retention:** Up to 12 months for:

- Ongoing investigations
- Legal proceedings
- Child protection cases
- Serious disciplinary matters

Secure Disposal: Certified data destruction after retention period

8.3 Breach Response

- Immediate containment and assessment procedures
- Notification to Information Regulator within 72 hours
- Communication to affected individuals where required
- Remedial action and system improvements
- Documentation and reporting requirements

---

9. GOVERNANCE AND OVERSIGHT

9.1 Management Structure

CCTV Manager: Principal (ultimate responsibility) **Deputy Manager:** Deputy Principal or designated senior staff member **Technical Administrator:** IT Manager or external service provider **Privacy Officer:** Designated staff member for privacy compliance

9.2 Regular Reviews

- **Monthly:** System functionality and maintenance checks
- **Quarterly:** Access logs and usage patterns review
- **Annual:** Full policy and procedure review
- **Incident-based:** Investigation of any misuse or breaches

9.3 Training and Awareness

- Mandatory training for all authorized personnel
- Annual refresher sessions on privacy and procedures
- Student and parent awareness programs
- Regular communication about surveillance practices

---

10. SIGNAGE AND NOTIFICATION

10.1 Warning Signs

Placement: Prominent signs at all main entrances and key locations **Content Requirements:**

- Clear CCTV symbol and text

Languages: English and other relevant community languages

10.2 Additional Notifications

- Website privacy notice with detailed information
- Parent handbook section on surveillance
- New student orientation materials
- Staff handbook provisions

---

11. COMPLAINTS AND APPEALS PROCEDURE

11.1 Internal Complaints

Step 1: Direct complaint to Principal (5 working days response)

Step 2: Appeal to School Governing Body Chair (10 working days)

Step 3: Final internal review by full Governing Body

11.2 External Appeals

- Information Regulator of South Africa
- Provincial Education Department
- Relevant professional bodies
- Legal proceedings (as last resort)

11.3 Complaint Handling

- Written acknowledgment within 2 working days
- Full investigation with independent review where appropriate
- Written response with findings and actions
- Follow-up to ensure complainant satisfaction

---

12. SPECIAL CONSIDERATIONS FOR EDUCATIONAL SETTINGS

12.1 Child Protection

- Enhanced safeguards for footage involving minors
- Restricted access protocols for child-related incidents
- Mandatory reporting obligations under Children's Act
- Specialized training for staff handling child-related footage

12.2 Educational Environment

- Minimal disruption to teaching and learning
- Respect for academic freedom and expression
- Protection of student-teacher relationships
- Support for positive school culture

12.3 Disciplinary Procedures

- CCTV evidence integration with school disciplinary policy
- Fair hearing procedures incorporating video evidence
- Appeal rights for disciplinary decisions involving CCTV
- Restorative justice approaches where appropriate

---

13. TECHNOLOGY UPGRADES AND FUTURE DEVELOPMENTS

13.1 System Enhancement

- Regular technology assessments and upgrades
- Privacy-enhancing technologies adoption
- Artificial intelligence and facial recognition considerations
- Integration with other school safety systems

13.2 Emerging Technologies

Prohibited Technologies (without specific policy amendment):

- Facial recognition systems
- Behavioral analytics software
- Tracking of individual movement patterns

Required Assessments for New Technology:

- Privacy impact assessment
- Necessity and proportionality review
- Community consultation
- Legal compliance verification

---

14. MONITORING AND EVALUATION

14.1 Key Performance Indicators

- Incident prevention and response times
- Successful investigations and resolutions
- Privacy compliance metrics
- Community satisfaction levels
- System reliability and uptime

14.2 Regular Audits

- Annual independent privacy audit
- Technical security assessment
- Policy compliance review
- Stakeholder feedback collection

---

15. POLICY REVIEW AND AMENDMENT

15.1 Review Schedule

- **Annual Review:** Comprehensive policy assessment
- **Legislative Changes:** Immediate review upon legal updates
- **Incident-Triggered:** Review following significant incidents

- **Technology Updates:** Assessment with system upgrades

15.2 Amendment Process

- Stakeholder consultation including parents and staff
- Governing Body approval for significant changes
- Legal review for compliance verification
- Community notification of policy changes

---

16. CONTACT INFORMATION AND RESOURCES

Policy Queries: Principal: Tim Stiff, Zandri Stiff - 0824468902

Complaints: School Office: As above

External Authorities: Information Regulator: www.justice.gov.za/inforeg/ Provincial Education Department:

---

17. POLICY ACKNOWLEDGMENT

All staff members, students, parents, and visitors are deemed to have read and understood this policy upon entering school premises. The policy is available in multiple formats and languages upon request.

Signed:
Principal
Date: 24 May, 2025

This policy reflects international best practices in educational surveillance while maintaining full compliance with South African law and respecting the rights and dignity of all school community members.