CCTV POLICY

Reviewed:	September 2025
Next Review Due:	August 2027
Applies To:	Whole School
Owner:	Head of School
Approved By:	Board of Directors

Mission, Vision and Values

Mission
To inspire our children to reach their full potential by fostering curiosity and an interest in learning, awakening their minds and illuminating their world.

Vision
To create an affordable international secondary school with a high standard of education where children learn through practical and project-based work. To develop our students' moral and intellectual capacity, and to encourage creativity and adaptability.

Aim
An education that is broad, balanced and challenging, with an emphasis on developing strong connections to our host country, Uganda.

Values
Desire for lifelong learning; an ability to adapt; be innovative and reflective thinkers; open minded, and empathetic while achieving high academic success according to individual potential.

7 HILLS INTERNATIONAL SCHOOL
ADVENTURE IN LEARNING

Contents

1. Purpose & Statement of Intent

2. Legal, Regulatory & Good Practice Framework

3. Scope

4. System Ownership & Management

4.1 Strategic oversight

4.2 Operational management

5. Location & Coverage

6. System Operation

7. Access Control & Authorised Users.

8. Storage, Retention & Security of Footage

9. Access, Disclosure & Subject Requests

10. Privacy, Safeguarding & DPIA

11. Faults, Maintenance & Security Assurance

12. Breaches, Complaints & Misuse

13. Monitoring & Review

14. Policy Review and Approval

15. Distribution and Access

1. Purpose & Statement of Intent

7Hills International School (7Hills) uses CCTV and surveillance systems to:

- promote a safe and secure environment for students, staff and visitors
- safeguard school property, facilities and assets
- deter and detect crime, vandalism and anti-social behaviour
- support incident investigation, safety management and emergency response
- assist law enforcement where appropriate
- support fair and transparent case-review and safeguarding processes

CCTV will not be used to:

- intrude unreasonably on personal privacy
- monitor normal student or staff activity
- observe teaching practice for performance management
- track specific individuals unless responding to a live safeguarding or safety concern
- capture images in areas where there is a heightened expectation of privacy (such as toilets, changing rooms, medical areas or counselling spaces)

The system is operated proportionately, ethically and in accordance with data-protection principles. CCTV footage will never be used for commercial or entertainment purposes.

2. Legal, Regulatory & Good Practice Framework

The policy follows relevant principles of:

- data protection, privacy and proportionality
- safeguarding and duty of care
- fair processing and transparency
- secure handling of recorded material
- evidential integrity and access control

It reflects good-practice guidance drawn from surveillance and school policy standards. Where local regulatory requirements apply, the school will comply with relevant national laws and guidance.

3. Scope

This policy covers:

- all CCTV cameras and recording devices on campus
- visual images and metadata captured by the system
- fixed, externally mounted and internal corridor cameras
- secure storage, retrieval and controlled disclosure of footage

It applies to:

- students and parents
- staff and contractors
- visitors and community users of the site

4. System Ownership & Management

The CCTV system is owned by 7Hills International School and operated under the authority of the Head of School.

4.1 Strategic oversight

- Head of School
- Board Finance, Governance & Risk Committee

4.2 Operational management

- ICT / Network Manager (system performance & security)
- Site & Facilities Manager (infrastructure / access control)
- Designated Safeguarding Lead (incident review where safeguarding applies)

Day-to-day operation may be delegated to authorised staff.

5. Location & Coverage

Cameras are located only where monitoring is required to achieve the stated aims.
Typical locations include:

- external gate and perimeter access points
- main entrances and reception areas
- corridors, stairwells and circulation spaces
- playgrounds, parking and campus grounds
- sports & shared-use external areas

Cameras will NOT be installed in:

- classrooms (except where required for security incident or examination monitoring)
- toilets
- changing rooms
- prayer/reflection rooms
- medical or counselling spaces

Clear and prominent signage will be displayed at all entrances to the school site and at appropriate locations throughout the campus wherever CCTV surveillance is in operation. The purpose of the signage is to ensure that students, staff, parents, visitors and contractors are aware that CCTV monitoring is taking place.

6. System Operation

- The system operates 24 hours a day, 365 days per year
- Cameras record visual images only (no audio capture)
- Time and date stamps are maintained and periodically checked
- Cameras are not directed at individuals except where immediate safety concerns require an urgent response

7. Access Control & Authorised Users

Access to live or recorded footage is strictly limited to authorised personnel and only where necessary for:

- safety or safeguarding review
- behaviour / incident investigation
- facilities or security risk assessment
- police or legal enquiry

Authorised staff may include:

- Head of School
- Designated Safeguarding Lead
- ICT / Network Manager
- Site / Facilities Manager
- Senior Leadership Team (where appropriate)

Visitors, contractors or third parties may not view images unless formally approved and supervised, and all access is recorded (see appendix 1).

8. Storage, Retention & Security of Footage

- Recordings are stored securely on encrypted servers or secure storage devices.
- Access requires individual login credentials.
- Server rooms and control equipment remain locked when unattended.

Retention

- Routine retention period: 30 days
- Footage required for investigation may be retained longer, then securely deleted.

Evidence copies are:

- sealed, logged, signed and stored securely
- only released to police or authorised legal requestors
- handled in accordance with evidential integrity procedures

9. Access to CCTV Footage

Access to CCTV footage is strictly controlled and will only be granted to authorised individuals for purposes consistent with the aims of this policy, including safeguarding, protecting students, staff

and visitors, preventing and investigating incidents, supporting disciplinary investigations, protecting school property, or where there is another lawful basis for access.

Every instance of viewing, downloading, copying or disclosing CCTV footage must be recorded in the school's CCTV Access Register (Appendix A). The register will include:

- Date and time of access
- Name and position of the authorised person
- Reason for accessing the footage
- Camera(s) or location viewed
- Incident or case reference (where applicable)
- Whether footage was copied or disclosed
- Authorising officer
- Signature or electronic approval

Visual display monitors used to view CCTV footage will be positioned in secure locations to ensure that footage cannot be viewed by unauthorised persons.

Authorised users are responsible for maintaining the confidentiality and security of all CCTV footage at all times.

9.1 Staff Access

Access to the CCTV system is restricted to staff whose responsibilities require it.

The following members of staff are authorised to access CCTV footage:

- Head of School
- Deputy Head of School(s)
- Designated Safeguarding Lead (DSL)
- Operations Manager
- ICT Manager/System Administrator
- Any member of the Senior Leadership Team specifically authorised by the Head of School
- Other staff authorised in writing by the Head of School for a specific purpose

CCTV footage may only be viewed using authorised school devices or designated secure monitoring stations.

All authorised users will receive appropriate training covering:

- operation of the CCTV system
- safeguarding responsibilities
- confidentiality
- data protection and privacy principles
- secure handling and disclosure of footage
- completion of the CCTV Access Register

Unauthorised access, disclosure, copying or misuse of CCTV footage will be treated as a serious disciplinary matter and may result in disciplinary action, referral to the appropriate authorities and, where applicable, legal proceedings.

9.2 Requests to Access Personal CCTV Footage

Individuals may request access to CCTV footage in which they appear, subject to applicable data protection legislation and the rights of other individuals.

Requests should be submitted in writing to the **Head of School** and should include sufficient information to enable the footage to be located, including where possible:

- date of the incident
- approximate time
- location
- description of the individual
- nature of the request

The school will acknowledge receipt of the request promptly and will normally respond within the timeframe required by applicable legislation.

Before releasing any footage, the school will verify the identity of the requester.

Where footage contains images of other identifiable individuals, the school will take reasonable steps to protect their privacy by:

- blurring or redacting identifying features;
- obtaining consent where appropriate; or
- providing still images or refusing disclosure where the privacy rights of others cannot reasonably be protected.

The school may refuse or partially refuse a request where disclosure would:

- prejudice an ongoing safeguarding, disciplinary or criminal investigation;
- compromise the privacy or rights of another individual;
- breach legal obligations; or
- otherwise be unlawful.

Where permitted by law, the school reserves the right to charge a reasonable administrative fee for manifestly unfounded, excessive or repetitive requests.

Approved footage will be shared securely using encrypted electronic transfer, password-protected files or another secure method determined by the school.

All disclosures will be recorded in the CCTV Footage Release Register (Appendix B).

9.3 Disclosure to Third Parties

CCTV footage will only be disclosed to third parties where there is a lawful and legitimate reason to do so, including but not limited to:

- safeguarding investigations;
- criminal investigations;
- requests from law enforcement agencies;
- legal proceedings;
- insurance investigations; or
- where disclosure is otherwise required or permitted by law.

Requests from external organisations should normally be submitted in writing to the Head of School.

The Head of School (or delegated senior leader) will determine:

- whether disclosure is lawful;
- the minimum amount of footage required;
- whether legal advice should be sought; and
- whether any redaction is necessary before disclosure.

Where the school receives a court order or other legally binding requirement to disclose footage, only the footage specifically required will be provided.

Every disclosure of CCTV footage will be recorded in the CCTV Footage Release Register, including:

- date of disclosure;
- recipient and organisation;
- lawful basis for disclosure;
- description of footage disclosed;
- authorising officer; and
- method of transfer.

Where footage is exported for safeguarding, disciplinary or criminal investigations, the school will maintain a clear chain of custody using the CCTV Evidence Handling Form (Appendix G) to ensure the integrity and admissibility of the evidence.

10. Privacy, Safeguarding & DPIA

CCTV deployment follows a privacy-by-design approach. Before installing, relocating or upgrading cameras, the school will:

- complete a risk-aware privacy / impact review
- consider safeguarding, cultural context and dignity
- ensure necessity and proportionality

11. Faults, Maintenance & Security Assurance

- Systems are checked routinely for performance and recording integrity.
- Faults are logged and repaired as soon as practicable
- Random operational checks may be conducted
- Cyber-security measures are applied to protect system access and stored data.

12. Breaches, Complaints & Misuse

Any misuse of CCTV systems or footage:

- will be investigated by the Head of School
- may result in disciplinary or legal action
- will be escalated where serious or deliberate

Complaints relating to CCTV will be managed under the school Complaints Policy.

13. Monitoring & Review

This policy and system operation will be reviewed:

- every two years, or
- following major incident, system upgrade or regulatory change

Effectiveness will be assessed against:

- safeguarding and safety outcomes
- proportionality and privacy impact
- operational reliability and governance controls

14. Policy Review and Approval

This policy will be reviewed annually or as required to reflect changes in legislation, CIS standards, or school practice.

15. Distribution and Access

This policy is available to all staff, students, and parents via the school website and on the school Google drive. Printed copies can be requested from the school reception.

Appendix A: CCTV Viewing Log

Date/Time	Person Accessing	Reason for Access	Footage Viewed	Any copies created	Any disclosures made

Appendix B: CCTV Footage Release Register

Date	Recipient	Basis for Disclosure	Description of Footage Disclosed	Authorised by	Method of Transfer

Appendix C – CCTV Camera Register – Operations Manager

	Camera ID	Location	Purpose	Coverage	Audio (Y/N)	Recording hours	Installation date	Last inspection

Appendix D – CCTV Annual Audit Checklist

Annual review of:

- cameras operational
- signage visible
- retention working
- access logs complete
- downloads logged
- passwords changed
- cyber security
- staff training completed
- policy review completed

Appendix E – Subject Access Request Form

Used when someone requests CCTV footage of themselves.

Includes:

- identity verification
- date/time
- location
- reason
- acknowledgement
- decision record

This is exactly the kind of appendix I would include in the policy. It's written in plain English for parents and should reduce many of the questions you receive after incidents.

Appendix F – Parent Guidance on the School's CCTV System

CCTV at 7Hills International School

The safety and wellbeing of our students, staff and visitors is our highest priority. As part of our safeguarding and security arrangements, 7Hills International School operates a CCTV system across selected areas of the campus.

This guide explains how CCTV is used and answers some of the questions parents commonly ask.

Why does the school use CCTV?

The school's CCTV system helps us to:

- safeguard students, staff and visitors;
- promote a safe and secure learning environment;
- prevent and deter bullying, violence, theft, vandalism and other inappropriate behaviour;
- investigate safeguarding concerns, behavioural incidents and accidents;
- assist emergency services or law enforcement where appropriate; and
- protect school buildings and property.

CCTV is one part of the school's wider safeguarding and security procedures and does not replace appropriate staff supervision.

Where is CCTV used?

CCTV cameras are located in public areas of the school where there is a legitimate safeguarding or security purpose, including entrances, exits, corridors, playgrounds, car parks and other communal spaces.

CCTV is **not** installed in areas where individuals have a reasonable expectation of privacy, such as toilets, changing rooms, shower facilities or counselling rooms.

Can parents ask to see CCTV footage?

Parents may request access to CCTV footage where there is a legitimate reason to do so and where the request relates to their child.

However, CCTV footage frequently captures images of several students, staff members and visitors. The school has a duty to protect the privacy and personal information of everyone recorded.

For this reason, parents are **not automatically entitled** to view or receive CCTV footage.

Each request is carefully considered on an individual basis.

Why can't the school simply share the footage?

Unlike a photograph of one individual, CCTV recordings often include multiple people.

Providing footage that identifies other students or staff could:

- compromise another child's privacy;
- breach data protection obligations;
- prejudice safeguarding, disciplinary or criminal investigations; or
- place individuals at unnecessary risk.

Even where an incident involves your child, the school may not be able to release the footage if doing so would affect the rights or safety of others.

When might CCTV footage be disclosed?

The school may disclose CCTV footage where there is a lawful and appropriate reason to do so, including:

- safeguarding investigations;
- school disciplinary investigations;
- police investigations;
- court proceedings;
- insurance investigations; or
- where disclosure is otherwise required by law.

Where footage is released, the school will only disclose the minimum amount of footage necessary and may blur or redact identifying features where appropriate.

How do I request CCTV footage?

If you believe CCTV footage may assist with an incident involving your child, please submit a written request to the Head of School.

Where possible, include:

- your child's name;
- the date of the incident;
- the approximate time;
- the location;
- a brief description of what happened; and
- why you believe the footage is required.

The school will acknowledge your request and consider it in accordance with its CCTV Policy and applicable data protection requirements

How long is footage kept?

Unless required for an ongoing safeguarding, disciplinary or legal investigation, CCTV recordings are normally retained for **30 days** before being securely deleted.

Requests should therefore be submitted as soon as possible following an incident.

Questions?

If you have any questions about the school's CCTV system or this guidance, please contact: Head of School