



مدرسة الآفاق الحديثة ذ.م.م.
NEW HORIZON SCHOOL W.L.L.

Page | 2

CCTV SURVEILLANCE, FOOTAGE ACCESS AND DISCLOSURE POLICY



INDEX

1. Purpose
2. Scope
3. Principles Governing CCTV Use
4. CCTV Camera Placement and Restrictions
5. Ownership and Responsibility
 - 5.1 Chairman / School Management
 - 5.2 Principal
 - 5.3 Designated CCTV Administrator / IT or Security Head
 - 5.4 Safeguarding Lead / Designated Safeguarding Personnel
 - 5.5 All Employees
6. Authorization to View CCTV Footage
7. Permitted Purposes for Viewing
8. Requests from Parents and Guardians
9. Requests from Employees
10. Requests from Police, Government Authorities or Other Third Parties
11. Footage Retention and Deletion
12. Confidentiality and Prohibited Activities
13. CCTV Footage Involving Student Safeguarding
14. Security, Storage and Technical Controls
15. CCTV Access and Disclosure Register
16. CCTV System Failure or Suspected Data Breach
17. Awareness and Signage
18. Policy Review and Compliance
19. Approval
- Appendix A: Forms and Registers required by the policy



CCTV SURVEILLANCE, FOOTAGE ACCESS AND DISCLOSURE POLICY

Policy Code: NHS/ADM/CCTV/01

Version: 1.0

Effective Date: October 2026

Review Date: October 2027

Policy Owner: Principal

Approving Authority: Chairman / School Management

Applicable To: All NHS campuses, employees, students, parents, visitors, security personnel and authorised service providers

1. Purpose

New Horizon School (NHS), Kingdom of Bahrain, is committed to maintaining a safe, secure and supportive learning environment. CCTV surveillance is used to support student safeguarding, prevent and investigate incidents, protect school property and assist in maintaining safety and security.

This policy establishes clear procedures governing CCTV monitoring, access to recordings, footage preservation, disclosure, confidentiality and accountability.

CCTV shall be used only for legitimate school purposes and in accordance with applicable Bahraini laws, Ministry of Education requirements and the school's safeguarding procedures.

2. Scope

This policy applies to all CCTV cameras, recording systems, storage devices, monitoring screens and associated footage operated or managed on behalf of NHS.

It covers:

- Entrances, exits, corridors, staircases, playgrounds, common areas and designated school facilities.
- School gates, parking areas and authorised transport-related areas.
- Any other location approved for CCTV installation following a legitimate safety or security assessment.

CCTV shall not replace active supervision by teachers, duty staff, counsellors, supervisors or security personnel.

3. Principles Governing CCTV Use

All CCTV operations shall follow these principles:



- 1. Safeguarding first: Student welfare and immediate safety take priority.**
- 2. Purpose limitation: Footage shall be accessed only for an authorised school-related purpose.**
- 3. Confidentiality: Recorded images shall be treated as confidential personal information.**
- 4. Restricted access: Only designated, authorised personnel may access the system.**
- 5. Proportionality: Surveillance shall be appropriate to the safety or security need.**
- 6. Accountability: Every footage review, export, disclosure and deletion override shall be documented.**
- 7. Fairness: Footage shall be assessed objectively and shall not be used to prejudice an individual.**

4. CCTV Camera Placement and Restrictions

Cameras may be installed in designated areas where monitoring is necessary for safety, safeguarding or security.

CCTV cameras shall not be installed in toilets, changing rooms, shower areas or other locations where individuals reasonably expect privacy.

Cameras shall not be used for covert monitoring of staff or students except where specifically lawful and formally authorised by the competent authority.

Audio recording shall not be enabled unless its necessity, lawfulness and any required approvals have been independently verified.

5. Ownership and Responsibility

5.1 Chairman / School Management

- Approves the policy and provides oversight.
- Ensures that appropriate security, staffing and technical resources are available.

5.2 Principal

- Acts as the policy owner and primary authorising authority for routine footage access.
- Approves footage reviews connected with school incidents and complaints.
- Ensures that safeguarding concerns are escalated through the established reporting system.
- Authorises preservation and disclosure in accordance with this policy and applicable law.
- Maintains oversight of the CCTV access register.

5.3 Designated CCTV Administrator / IT or Security Head

- Maintains the CCTV system, user permissions and recording functionality.
- Ensures that footage is stored securely and access credentials are protected.
- Provides footage only upon documented authorisation.



- Maintains access, export and technical incident logs.
- Reports system failures, unauthorised access and suspected data breaches immediately.

5.4 Safeguarding Lead / Designated Safeguarding Personnel

- Coordinates safeguarding-related footage requests with the Principal.
- Ensures that footage relevant to an allegation or reportable incident is preserved promptly.
- Coordinates with the appropriate authorities where required.

5.5 All Employees

- Must not access, photograph, record, download, copy or share CCTV footage without authorisation.
- Must report any suspected incident, safeguarding concern or CCTV-related breach immediately.

6. Authorisation to View CCTV Footage

All routine requests to view CCTV footage must be submitted to the Principal or the formally designated authorised officer.

The request must specify:

- Date and approximate time of the incident.
- Location or camera reference, where known.
- Reason for the request.
- Incident report or complaint reference, if applicable.
- Name and designation of the person requesting access.

The Principal shall determine whether the request is necessary, proportionate and appropriate.

The Principal may authorise the designated CCTV Administrator to retrieve footage and arrange a controlled review. The administrator shall not independently decide whether footage may be disclosed.

In the Principal's absence, the formally designated acting authority may approve urgent access, subject to documentation and subsequent review.

7. Permitted Purposes for Viewing

CCTV footage may be reviewed when reasonably necessary for:

- Student injury, accidents or medical emergencies.
- Bullying, physical altercations, harassment or suspected misconduct.
- Student safeguarding and child-protection concerns.
- Missing students, unauthorised departures or access-control incidents.
- Damage to school property, theft or security incidents.
- Complaints involving conduct within CCTV-monitored areas.
- School transport or campus safety incidents, where relevant footage is available.
- Official investigations or lawful requests from competent authorities.



- Verification of facts where a documented school-related concern warrants review.

CCTV footage shall not be reviewed out of curiosity, for personal reasons, or to monitor individuals without a legitimate and authorised purpose.

8. Requests from Parents and Guardians

Parents or guardians may submit a written request to the Principal when CCTV footage may be relevant to an incident involving their child.

The request should include the child's name, class, date, approximate time, location and nature of the concern.

Upon receiving the request, NHS shall:

- 1. Acknowledge and register the request.**
- 2. Assess the incident and identify relevant footage, if available.**
- 3. Preserve relevant footage where necessary.**
- 4. Review the request in accordance with safeguarding, confidentiality and applicable data-protection requirements.**
- 5. Communicate the decision and any appropriate next steps to the parent or guardian.**

Parents do not have an automatic right to receive a copy of CCTV footage or to view recordings containing other students, employees or visitors.

Where disclosure is legally permissible and appropriate, NHS shall consider whether the request can be accommodated through a controlled viewing, a suitably redacted copy or another appropriate means.

The school shall not promise unrestricted access to footage or disclose recordings without considering the rights and safety of everyone identifiable in them.

9. Requests from Employees

Employees may submit a written request for CCTV review concerning a specific workplace incident, safety concern or formal complaint.

The Principal or authorised officer shall consider the request objectively and in accordance with applicable law and school procedures.

Employees shall not access CCTV systems directly or use footage obtained through unofficial means.

Where an employee is the subject of a formal investigation, the school shall follow applicable employment procedures and provide any disclosure or opportunity to respond that is legally required.



10. Requests from Police, Government Authorities or Other Third Parties

Requests from the Ministry of Education, police, courts or other competent authorities shall be referred to the Principal or the formally authorised school representative.

NHS shall verify the identity and authority of the requester, document the request and assess the applicable legal requirements.

Where a valid legal obligation or lawful direction requires disclosure, the school shall cooperate within the scope of that obligation.

Footage shall be provided securely, with an appropriate record of the recipient, date, purpose and material disclosed.

Requests from lawyers, insurance companies, transport operators, other schools or private individuals shall be assessed separately. Such requests do not, by themselves, authorise disclosure.

11. Footage Retention and Deletion

CCTV footage shall be retained only for as long as necessary for the school's documented security and safeguarding purposes, subject to applicable legal requirements and any required approvals.

Proposed NHS operational standard: Routine footage may be retained for up to 120 days, provided this period is consistent with applicable law, required approvals, storage arrangements and the school's documented assessment.

Footage relevant to an accident, safeguarding concern, complaint, investigation, legal claim or official request must be preserved before routine deletion, where lawful and necessary.

Preserved footage shall:

- Be isolated from routine deletion.
- Be accessible only to authorised personnel.
- Carry a case reference and preservation date.
- Be reviewed periodically to determine whether continued retention remains necessary.
- Be securely deleted when the preservation purpose ends and no further legal or safeguarding requirement applies.

The 120-day period is a proposed internal standard, not a claim that Bahraini law mandates that specific retention period.

12. Confidentiality and Prohibited Activities

The following activities are strictly prohibited:

- Recording CCTV screens using a personal mobile phone.
- Sharing footage through WhatsApp, personal email, social media or other unauthorised channels.
- Posting footage or screenshots in staff groups, parent groups or public forums.
- Downloading, editing, deleting or copying footage without permission.
- Using footage for personal disputes, gossip, humiliation or retaliation.



- Providing passwords or system access to unauthorised persons.
- Altering, concealing or destroying evidence relating to a reported incident.

Any suspected breach shall be reported immediately to the Principal and investigated in accordance with school procedures. Appropriate disciplinary, contractual or legal action may follow, subject to applicable law.

13. CCTV Footage Involving Student Safeguarding

Where footage indicates possible abuse, bullying, assault, serious misconduct or another student-protection concern:

1. Ensure the immediate safety of the student or other person at risk.
2. Notify the Principal and designated safeguarding personnel immediately.
3. Record the concern using the school's approved incident-reporting procedure.
4. Preserve the relevant footage promptly and restrict access.
5. Avoid unnecessary repeated viewing, informal questioning or circulation of the recording.
6. Follow applicable Ministry of Education reporting requirements and directions from competent authorities.
7. Maintain a documented record of all actions taken.

CCTV footage is supporting evidence and shall not be treated as the sole determinant of whether an allegation is true or false.

The school shall not delay an urgent safeguarding referral while waiting for CCTV footage to be retrieved.

14. Security, Storage and Technical Controls

The school shall implement appropriate safeguards, including:

- Password-protected systems and role-based access.
- Secure storage and protection against unauthorised copying or alteration.
- Restricted physical access to recording equipment.
- Appropriate network security and authorised remote-access controls.
- Periodic checks of camera functionality, system clocks and recording availability.
- Secure transfer procedures for approved footage exports.
- Prompt reporting and investigation of suspected data breaches.

Any external CCTV service provider shall be subject to appropriate confidentiality, security and data-processing obligations.

15. CCTV Access and Disclosure Register

The CCTV Administrator shall maintain a register containing:



- Serial number of the request.
- Date and time of request.
- Requester's name and designation.
- Incident reference and stated purpose.
- Relevant camera, date and time range.
- Name of the approving authority.
- Names of personnel who viewed the footage.
- Whether footage was exported, disclosed or preserved.
- Recipient and legal basis for any disclosure.
- Date and method of transfer.
- Retention or deletion review date.
- Remarks and follow-up actions.

The Principal shall review the register periodically and investigate any unexplained access or discrepancies.

16. CCTV System Failure or Suspected Data Breach

A camera failure, recording interruption, unauthorised access, loss of footage or suspected disclosure shall be reported to the Principal immediately.

The school shall assess the seriousness of the incident, preserve available evidence, restrict compromised access where necessary and implement corrective action.

Where applicable, notification to the relevant authority or affected individuals shall be made in accordance with Bahrain's legal requirements.

17. Awareness and Signage

Appropriate notices shall inform students, parents, employees and visitors that CCTV surveillance operates in designated areas.

The notices and associated privacy information shall explain the purpose of surveillance, the responsible school contact and how to submit a request or raise a concern.

Employees shall receive appropriate guidance on CCTV confidentiality, safeguarding escalation and access restrictions.

18. Policy Review and Compliance

This policy shall be reviewed annually or earlier if there is a change in legislation, Ministry of Education requirements, CCTV technology or safeguarding procedures.

Any breach shall be addressed in accordance with applicable school policies, employment requirements and Bahraini law.

The policy shall be read alongside the NHS Student Safeguarding Policy, Incident Reporting Procedure, Staff Code of Conduct, Data Protection requirements and applicable Ministry of Education directives.



مدرسة الآفاق الحديثة ذ.م.م. NEW HORIZON SCHOOL W.L.L.

Page | 2

19. Approval

Prepared by: Principal, New Horizon School

Reviewed by: School Management / Designated CCTV Administrator

Approved by: Chairman / Authorised School Management Representative

Signature: _____

Date: _____

Effective from: _____



مدرسة الآفاق الحديثة ذ.م.م. NEW HORIZON SCHOOL W.L.L.

Page | 2

APPENDIX A — IMPLEMENTATION FORMS AND REGISTERS

The following controlled forms and registers support implementation of this policy.

- Form 1 — Internal CCTV Footage Access / Review Request
- Form 2 — Parent / Guardian CCTV Footage Request
- Form 3 — Employee CCTV Footage Request
- Form 4 — Police / Government Authority / Third-Party Request Record
- Form 5 — CCTV Footage Preservation and Retention Review
- Form 6 — CCTV Access, Export and Disclosure Register
- Form 7 — CCTV System Failure / Suspected Data Breach Report
- Form 8 — CCTV Camera and Recording System Check
- Form 9 — CCTV Footage Deletion / Disposal Record