POLRM003/GEMS CCTV and Surveillance Policy	
Policy Title:	**GEMS CCTV and Surveillance Policy**
Policy Number:	POLRM003
Version:	V2
Effective date:	June 2024
Scheduled review date:	June 2026
Policy approver:	Risk and Compliance Committee
Policy owner:	Chief Risk and Compliance Officer & SVP Government Relations and Safecor
Relevant related policies:	POLCSG001 Safeguarding Policy POL/HR0008 - Employee Code of Conduct POL/QHSE21 Incident Investigation POL/QHSE39 Occupational Health and Safety (OHS) POL/QHSE40 Quality Policy POL/QHSE41 Emergency Response Plan POL/QHSE42 Pool Standard Operating Procedure (PSOP) Safecor Security Handbook Respective Manuals

1 Policy scope and purpose

Application

1.1 This policy applies to GEMS MENASA Holdings Limited (the "Company" or "GEMS") and its subsidiaries and subsidiary undertakings (together with the Company, the "Group", and any of them, a "Group Company"), which includes:

a. All schools and businesses within UAE and Qatar; and

b. All of those who represent the Group in any capacity, including agents, sponsors, intermediaries, representatives, finders, and introducers.

Purpose

1.2 The purpose of this policy is to set out minimum standards for use and management of Closed-Circuit Television ("CCTV") systems and associated technologies within GEMS.

1.3 For the purposes of this policy, CCTV system includes:

a. Video capture equipment, such as cameras.

b. Video Management Software (VMS), including any apps used to access CCTV footage.

c. Video display equipment, whether fixed (screens) or portable (laptop, tablet etc.); and

d. Hardware equipment to support CCTV, such as servers and storage.

1.4 This policy is based on regulatory guidelines in UAE, international standards, such as ISO:9001 and ISO:14001 and our understanding of business needs.

1.5 This is an overarching, group-wide policy. In case a local policy is in place in a country or in one of the businesses within GEMS (e.g. STS), the stricter of the group and local policy will apply.

2 Central policy statements and requirements

Use of CCTV

2.1 GEMS has a corporate and regulatory responsibility to safeguard its students and to provide a safe and secure environment for its employees and visitors. GEMS utilizes CCTV systems and associated monitoring and recording equipment to meet these obligations. Specifically, GEMS uses CCTV systems to ensure:

a. The promotion of a safe learning environment.

b. The safety and wellbeing of students, staff, visitors, and contractors while protecting individual privacy at all times.

c. The prevention and detection of crime, vandalism, unlawful behavior, and inappropriate conduct.

d. The protection of buildings, offices, facilities, and assets within.

2.2 CCTV systems will be used in a confidential, ethical, and legal manner. Specifically, CCTV systems will not be used to:

a. Provide recorded images for internet advertising or marketing purposes.

b. Monitor staff productivity or performance.

c. Conduct academic evaluations of students.

d. Monitor private properties or residential areas around schools.

e. Record audio without explicit consent and

f. Violate any known and applicable laws, regulations, or ethical standards.

2.3 This policy prohibits monitoring based on characteristics and classifications of the subject e.g. race, gender, ethnicity etc.

2.4 GEMS will not engage in any covert surveillance. To this end, cameras must always be visible, and the use of CCTV must be sign-posted.

Coverage

2.5 CCTV cameras should cover both internal and external areas at the respective location.

2.6 Coverage and location of the cameras must be as per the regulations for each Emirate (included with Appendix 7A), however, should at least cover:

a. All entrances and exits of the buildings and grounds, including parking.

b. All walkways and common areas such as corridors, stairs, courtyard, sports hall, sports fields, canteen, labs, libraries, entrance to washrooms (avoiding inside areas) and elevators etc.

c. Service rooms (electrical room, pump room etc.), student pickup and drop-off areas.

d. Sensitive areas, such as CCTV control room, cash handling areas, server rooms etc.

e. Exterior areas surrounding the perimeter of the building.

2.7 CCTV cameras should not be installed in areas where there is a reasonable expectation of privacy, such as lavatories, changing rooms and prayers rooms. For avoidance of doubt, swimming pools are considered public places for the purposes of this policy.

Access and Monitoring

2.8 For the purposes of this policy, "Access" refers to having the ability to view video recording or historical footage, while 'Monitoring' refers to the ability to view live footage.

2.9 Access to the CCTV system and stored images must be restricted to authorized individuals only. For this purpose and in context of this policy, authorized individuals include:

a. CEO/Principal/Superintendent

b. Manager School Operations (MSO)

c. Designated security or other staff approved by CEO/Principal or Managing Director, Safecor

2.10 From time to time, the Chief Risk and Compliance Officer, Chief Audit Executive, SVP Government Relations and Safecor, Corporate Head of Safeguarding and Group Health and Safety (HSE) Manager may require access to school CCTV system as part of investigations, audits or other purposes. In such instances, it is expected that the School Principal will be informed in advance by the concerned party.

2.11 In circumstances where sensitive or explicit content is likely to have been captured by CCTV, the Principal is required to take steps to manage and limit access to such footage.

2.12 School ICT engineer(s) will be granted admin access to all components of the CCTV infrastructure to facilitate L1 IT support. In addition, nominated and licensed CCTV vendors will have admin access to VMS to facilitate L2/L3 support and maintenance for overall CCTV services.

2.13 Access privileges to the CCTV system must be reviewed and signed off bi-annually by the respective School Principal.

2.14 Access to CCTV footage must only be made available through a secure, password protected GEMS machine or platform. In case of access through an application, the application must be access controlled, with a CCTV user profile, username, and password.

2.15 Portable devices, such as tablets, laptops, mobile phones etc. must not be

used to access CCTV footage in normal course. Only dedicated systems connected to wired network should be used to access CCTV systems.

2.16 Passwords for CCTV Infrastructure should adhere with the GEMS Password Policy.

2.17 Monitoring of CCTV footage should be restricted to authorized individuals only and should be away from public view. For this purpose:

a. It is preferred for the school to have a dedicated command and control center. However, in the absence of this or in addition to this, monitors can be installed in the office of the Principal or MSO.

b. Other monitors may be installed as needed for access by security guards for the purpose of monitoring the facilities outside of school hours and overnight. However, these must be a in secure room behind a lockable door.

2.18 School CCTV Systems (at least main points of entrance and exit) may be connected to the central Safecor control center for monitoring purposes. This is recommended for all premium schools in the GEMS network.

Access or Information Request

2.19 Access or information requests for CCTV can only be made by company staff (school management, teachers etc.). Under any circumstance, access requests from parents or members of the public should not be accepted.

2.20 Access or information request must be made in writing in the prescribed format (included in Appendix 7B) to any one of the authorized individuals along with rationale for the request.

2.21 CCTV footage should be accessed for serious incidents, such as safeguarding incidents, physical assaults, incidents leading to injuries etc. Use of footage for minor incidents is discouraged. However, it is ultimately at the discretion of authorized individuals to determine whether it is appropriate to allow access to CCTV footage or not.

2.22 Footage or information obtained through the CCTV system must only be released after approval from an authorized individual.

2.23 Depending on the perceived sensitivity of the content, either the individual requesting access can view the footage alongside an authorized individual, or an authorized individual can view the footage and provide a description of events, verbally or in writing.

2.24 Staff should ensure that there is evidence of request from regulatory authorities (such as KHDA) or law enforcement agencies (such as Dubai Police) prior to the release of CCTV footage to the authorities or agencies.

Operational Requirements

2.25 The CCTV system should be operational 24 hours a day, 365 days a year.

2.26 The CCTV system must record footage on a continuous basis.

2.27 The equipment must be according to the technical specifications required in each Emirate.

Retention, deletion, and transfer

2.28 CCTV footage must be retained for at least 60 days or for longer as guided by local regulatory requirements. Specifically, footage must be retained for:

Jurisdiction	Retention Requirement
Dubai & Sharjah	60 days
Abu Dhabi & Northern Emirates	90 days
Qatar	120 days

2.29 CCTV footage must not be tampered with or deleted. If this is deemed necessary, prior exceptional approval is required from Chief Disruption Officer and Chief Risk and Compliance officer. Legal opinion should be sought and must accompany such requests for exceptional approval.

2.30 Any request for transfer of CCTV footage off GEMS systems must be approached with extreme caution and must not be executed without written approval from an authorized individual. As such, a transfer of CCTV footage to non-GEMS systems is only permitted at the request of regulatory authorities or law enforcement agencies. All other requests are strictly prohibited.

2.31 The following waterfall approach should be adopted in response to requests from regulatory authorities for viewing or transfer of CCTV footage:

a. CCTV footage should be viewed on GEMS approved device / platform at GEMS premises. If this isn't acceptable then;

b. CCTV footage should be viewed on a GEMS device at the premises of the relevant authority. If this isn't acceptable then;

c. Temporary and read-only access should be granted to a named individual and via a specified email address or username. If this isn't acceptable then as a last resort;

d. CCTV footage can be provided in a downloadable format on a password protected storage device, such as a USB.

Maintenance

2.32 The maintenance of the CCTV system must be frequent and rigorous to ensure that it is operational at all times. Any disruption to or malfunction in CCTV systems must be reported to an authorized individual.

2.33 Annual Maintenance Contracts (AMC) are mandatory for CCTV systems. Central procurement process must be followed to procure AMC.

2.34 Service Level Agreement (SLAs) must exist between school management and the provider of AMC for each school. Such agreements / contracts should be reviewed by Safecor and SSC IT teams before the effective date.

2.35 Health checks of the CCTV infrastructure must be carried out at least annually. Such health checks must be conducted by suitably qualified personnel.

2.36 Fault detection mechanisms must be employed to detect and report, through

alerts, any CCTV related faults including availability or hardware issues.

2.37 CCTV software and firmware must be kept up to date at all times with latest patches and updates.

2.38 Issues pertaining to the CCTV system, including downtime or outages, must be reported promptly to the authorized individuals.

Data Privacy

2.39 Recognizable images captured by CCTV systems are "personal data." These are therefore governed by appropriate GCC federal law around the privacy and protection of personal data.

2.40 As a minimum, personal data must only be retained for the purpose and timeframe it's required for and must be deleted after this purpose is met.

2.41 Personal data must not be used or transferred without the subject's express consent.

2.42 Access to the CCTV system and stored images will be restricted to authorized individuals only.

Risk Assessment

2.43 A risk assessment of the school CCTV systems must be conducted on a periodic basis, but no later than 6 months from the beginning of the school term, by a central (e.g. Safecor) or an independent service provider.

2.44 Key findings and issues from the CCTV risk assessment report must be shared with the CEO/Principal and the School MSO. Any high-risk issues should also be reported to the Risk Management function.

2.45 Key findings from the CCTV risk assessment report must be acted upon and closed according to the timeframes specified within the risk assessment report. Any exception or risk acceptance pertaining to key findings must be approved by the school CEO/Principal.

3 Roles and responsibilities

Chief Executive Officer (CEO)

3.1 The CEO is responsible for:

a. Ensuring that due importance is placed on adherence to risk management policies including the GEMS CCTV and surveillance policy.

b. Ensuring that in conjunction with the Chief Risk and Compliance Officer, this policy is communicated to all relevant areas of the business.

c. Reviewing and opining on any exceptional approvals in conjunction with relevant functions.

Chief Risk and Compliance Officer (CRCO):

3.2 GEMS CRCO is responsible for ensuring that:

a. This policy remains appropriate for business and is in line with regulatory requirements and guidelines.

b. This policy is communicated to all relevant stakeholders within GEMS and guidance is provided in relation to implementation of the policy.

c. Any risks highlighted by schools and / or other central functions (such as IT, Safecor etc.) pertaining to the CCTV systems are understood, assessed, and managed.

d. Highlight material risks pertaining to TV systems at GEMS to the CEO and / or the Board Risk and Audit Committee.

School CEO/Principals:

3.3 Under this policy, the School Principal is required to ensure that:

a. All aspects of the policy are adhered to and in case of any exceptions, approvals are sought in accordance with this policy and are kept on record.

b. In addition to the policy, CCTV system complies with any additional Emirate-specific laws and regulations in relation to CCTV and surveillance systems.

c. The CCTV system remains operational at all times and any preventive maintenance is carried out in a timely manner.

d. List of authorized individuals is clear and that authorized individuals are adequately trained in the use and management of the CCTV system commensurate with their role.

e. Access to CCTV is limited to authorized individuals only and the information request process for other staff is rigorously followed.

Manager of School Operations (MSO):

3.4 The MSO is envisaged to be the overall custodian for CCTV systems at schools and the central point of contact for all aspects related to CCTV system in the school. Specifically, the MSO is required to ensure that:

a. All aspects of CCTV policy are implemented within the school and any exceptions are brought to the attention of the Principal.

b. Any incidents requiring viewing, extraction and sharing of CCTV footage are handled in line with this policy.

c. CCTV coverage in school remains appropriate for the school's needs.

d. Annual Maintenance Contracts (AMC) are in place and renewals are planned with relevant central departments (procurement, finance etc.) as part of the relevant cycle.

e. The school CCTV system continues to operate effectively, and any glitches or outages are promptly resurrected in conjunction with the maintenance partner.

f. All patches and updates are deployed by the maintenance partner in a timely manner.

g. CCTV fault detection mechanisms are deployed and maintained by the vendor to ensure that functionality exists to identify and report faults.

h. Recommendations in the security risk assessments performed by SAFECOR or other security agencies are reviewed, assessed, and resolved working in conjunction with the Principal and other relevant members of the school SLT.

SVP Government Relations & Safecor / Managing Director Safecor (Collectively "Safecor Leadership")

3.5 Safecor leadership is required to:

a. Ensure that procedures to operationalize this policy are developed and disseminated to all schools.

b. Ensure that security personnel are trained and licensed in the proper use and monitoring of CCTV systems.

c. Work closely with MSO to ensure that school security strategies align with this policy and requirements outlined within Safecor security handbook.

d. Oversee central CCTV monitoring operations at SSC.

e. Facilitate communication and cooperation with law enforcement agencies and other relevant authorities, as required.

Security Head Guard/CCTV Operator (Collectively "Collectively Security Personnel")

3.6 Respective Security Personnel are required to:

a. Monitor live footage and report any suspicious activities to the MSO.

b. Ensuring appropriate use of the CCTV system and ensuring that security and confidentiality procedures are followed at all times.

c. Conduct regular inspections to ensure that CCTV system continues to operate as expected.

d. Report any faults, including downtime or outages, to the MSO.

Enterprise Risk Management

3.7 Enterprise Risk Management department is responsible for:

a. Assessing, via reports from MSO and / or risk assessment reports, the potential risks associated with the use of CCTV systems, such as privacy concerns, data breaches, equipment failures, and legal compliance issues.

b. Ensuring that plans exist to remedy risks and / or issues associated with the school CCTV systems and overseeing the implementation of such plans.

c. Escalate any material risk associated with CCTV systems Board Risk and Audit Committee.

d. Providing internal consultancy and guidance to business units on compliance with CCTV policy.

GEMS Central Technology (SSC IT)

3.8 Central Technology teams (SSC IT) are responsible for:

a. Developing an overall strategy for the specifications of CCTV systems within GEMS including the direction for use of servers, storage, and other equipment.

b. Providing guidance and technical assistance to MSOs on the specification and selection of CCTV technology in accordance with related laws and regulations.

c. Assisting in upgrading of CCTV systems and managing technology shift in collaboration with school management.

d. Supporting with forensic/specialized investigations at the request of an authorized individual or GEMS Management.

Health and Safety Team (HSE)

3.9 The central HSE team is responsible for reviewing the effectiveness of controls and procedures governing the use of CCTV systems, including access controls, data protection measures, and incident response protocols.

Procurement

3.10 Procurement department is responsible for:

a. Sourcing competitive quotes for the deployment, management and maintenance of CCTV systems and associated equipment at the request of school MSOs or SSC IT.

b. Negotiating contracts with vendors ensuring cost-effective purchasing, overseeing the procurement process, and ensuring compliance with technical and regulatory standards.

Finance

3.11 Finance department is responsible for:

a. Overseeing the development of annual budgets (CAPEX and OPEX) covering operational maintenance, system renewal, and any additional expenditures pertaining to CCTV systems.

Internal Audit

3.12 Internal Audit team is responsible for:

a. Conducting periodic audits of CCTV systems and related processes to ensure compliance with company policies, industry standards, and regulatory requirements.

b. Providing reports and updates directly to the Board if there is a significant change on the status of CCTV operations, compliance issues, and audit findings.

4 Compliance with this policy

4.1 All schools and business units within GEMS are expected to comply with all aspects of this policy.

4.2 Where day one compliance is not possible or achieved, a glide path to compliance is required and expected.

Obligation to report non-compliance with this policy

4.3 All Personnel who suspect or become aware of any non-compliance with this policy have an obligation to report this promptly. Reporting can be made via the following routes:

a. For GEMS Personnel, to the relevant individual's line manager.

b. To the Compliance department (compliance@gemseducation.com).

c. Through the Group's anonymous Whistle-blower hotline (contact details provided below), in accordance with the Group's ***Whistle-blowing Policy POL/HR0014***.

Channel	Contact details
Toll free number	8 00 032 0827 (UAE) / 00800 100 702 (Qatar)
Email address	report@speak-safe.com
Website	http://www.speaksafe.whispli.com/kpmg
Surface mail	Speak-Safe Whistleblower Mailbox, P.O. Box 3800, Dubai

Investigation of reports of non-compliance

4.4 Reported allegations of non-compliance with this policy will be considered and, if appropriate, investigated by the Company.

4.5 Unless otherwise directed by the GEMS Board or Board Risk & Audit Committee, the Chief Audit Executive (in conjunction with the Internal audit department, legal department or any other department, as required) is responsible for initiating and overseeing any internal investigation of reports of non-compliance with this policy.

4.6 The Chief Audit Executive shall, at periodic intervals, make arrangements for audit of compliance against the requirements of this policy on an office and function basis. The results of such audits shall be reported to the Risk & Audit Committee of the Board.

5 Staff awareness and training

5.1 Any individual, whether they are an employee, contractor, or otherwise must familiarize themselves with this policy.

5.2 Individuals assigned as security personnel or CCTV operators must undergo relevant internal and / or external training and, when deemed necessary, obtain licensing sanctioned by the appropriate governing bodies. Furthermore, meticulous documentation of all licensing and training resources is imperative to facilitate prompt and thorough responses to inquiries from regulatory entities.

5.3 The Group will make this policy available on the Company's intranet for all Personnel.

The policy was reviewed by the following members of the GEMS management team.

No.	Name	Designation
1.	Dr. Saima Rana	Chief Education Officer
2.	Zafar Raja	Chief Operating Officer
3.	Krishan Gopi	Chief Disruption Officer
4.	Basel Ahmed	Chief Audit Executive
5.	Jake Barnard	General Counsel
6.	Steve Burnell	Executive Director, Health and Safety
7.	Claire Scowen	Corporate Head of Safeguarding
8.	Aamir Bukhari	Managing Director, Safecor

6 Appendices

A. Emirates-specific guidelines for CCTV Management

Emirates	Specific Regulation	Related Document Link
Dubai	SIRA Standard and Technical Specifications of the Security Systems (2018)	Document link
Abu Dhabi	Manual of Standards For Surveillance 2023	Document Link
Sharjah	Critical Infrastructure Security Technical Guideline	Document Link
Fujairah	Fujairah's Technical Specifications of CCTV Surveillance Cameras and Security System (2018)	Document Link
Ras Al Khaimah	Ras Al Khaimah Himaya Technical Regulations of the Supported Security at the Facilities and Public Events	Document Link
Qatar	Law No. 9 of 2011 regulating the use of Security and Surveillance CCTV Camera and devices	Document Link

B. Access or Information Request form – CCTV

The following form should be used to make an access request for CCTV:

Applicant Information	
Full Name	
Position/Role	
Department/Organization	
Contact Information (Phone Number & Email)	
Reason for Access or Information Request	
Purpose of the Request (e.g., security investigation, incident review, compliance check)	
Reason for Access or Information Request	
Date(s) of the Footage	
Time Frame(s) of the Footage	
Location of the Cameras (specific areas or Camera IDs)	
Description of the Event or Incident	

Confidentiality and Compliance Statement of Applicant and Approver	
I acknowledge that the CCTV footage requested contains confidential information and will be handled in strict accordance with applicable privacy and data protection laws. I understand that unauthorized access, use, disclosure, or distribution of this footage is prohibited and may result in disciplinary action and/or legal consequences. I agree to maintain the confidentiality of the footage and use it solely for the stated purpose. I agree to comply with GEMS CCTV and Surveillance Policy and all relevant policies, procedures, and regulations regarding the use and management of CCTV footage as outlined by GEMS and applicable laws.	
Applicant	**Approved By**