Dunes International School
Plot no 19; Shabiya 9; Mussafah; Abu Dhabi; P.O Box 5121
Tel.: 0097125527527
School code: 90201 | Affiliation number: 6630051

مدرسة ديونز الدولية
رقم قطعة: ١٩, شعبية ٩, مصفح, أبوظبي, ص ب : ٥١٢١
هاتف: ٠٠٩٧١٢٥٥٢٧٥٢٧
كود المدرسة : ٩٠٢٠١ | رقم الانتساب: ٦٦٣٠٠٥١

POLICY ON CLOSE CIRCUIT TV

Introduced:	March, 2019
Review 1:	March 2021
Review 2:	March 2023
Next Review :	March 2026

DEFINITION:

CCTV (closed-circuit television) is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes.

PURPOSE:

Dunes International School seeks to ensure the security and safety of all students, staff, visitors, contractors, its property and premises.
Therefore DIS has deploys CCTV monitoring in accordance with The Monitoring and Control Center ("MCC") - established by the Executive Council of the Emirate of Abu Dhabi under Abu Dhabi Law No.5 of 2011 ("MCC Law") with the statutory aims to:

- promote a safe environment and to monitor the safety and security of its premises;
- assist in the prevention, investigation and detection of crime;
- assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings; and
- assist in the investigation of breaches of its codes of conduct and policies by staff, students and contractors and where relevant and appropriate investigating complaints.

POLICY:

- The CCTV systems installed in and around Dunes International School cover building entrances, perimeters, external areas such as play grounds, swimming pool, internal areas such as reception lobby, computer rooms, rooms with high value equipment, some corridors and class rooms. They continuously record activities in these areas
- CCTV Cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities etc.

- CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed where relevant, so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV.

Covert recording

- Covert recoding i.e. recording which takes place without the individual's knowledge
- May only be undertaken in exceptional circumstances, for example to prevent or detect an unlawful act or other serious misconduct, and if is proportionate i.e. there is no other reasonable, less intrusive means of achieving those purposes;
- May not be undertaken without the prior written authorisation of the Principal and Admin Officer. All decisions to engage in covert recording will be documented, including the reasons;
- Will focus only on the suspected unlawful activity or suspected serious misconduct and information obtained which is not relevant will be disregarded and where reasonably possible, deleted;
- Will only be carried out for a limited and reasonable period consistent with particular purpose of the recording and will not continue after the investigation is completed.

Control room

No unauthorised access to the Security Control Room ("the Control Room") will be permitted at any time.

Other than Security Control Room Staff, access to the Control Room will be limited to:

• Persons specifically authorised by the Safety officer/ Principal;
• Security Supervisor;
• Security Control Room Operator;
• Maintenance engineers;
• police officers where appropriate; and
• Any other person with statutory powers of entry.

Monitors are not visible from outside the Control Room.

Before permitting access to the Control Room, security staff will satisfy themselves of the identity of any visitor and existence of the appropriate authorisation. All visitors are required to complete and sign the visitors' log, which includes details of their name, department and/or the organisation that they represent, the person who granted authorisation and the times of entry to and exit from the Control Room. A log of shall be retained setting out the following:

• Person reviewing recorded footage;
• Time, date and location of footage being reviewed; and
• Purpose of reviewing the recordings.

Processing of Recorded Images

CCTV images will be displayed only to persons authorised to view them or to persons who otherwise have a right of access to them. Where authorised persons access or monitor CCTV images on workstation desktops, they must ensure that images are not visible to unauthorised persons for example by minimising screens when not in use or when unauthorised persons are present. Workstation screens must always be locked when unattended.

Quality of Recorded Images

Images produced by the recording equipment must be as clear as possible so they are effective for the purpose for which they are intended. The following points to be taken care of

• Recording features such as the location of the camera and/or date and time reference must be accurate and maintained;

• Cameras must only be situated so that they will capture images relevant to the purpose for which the system has been established;

• Consideration must be given to the physical conditions in which the CCTV cameras are located i.e. additional lighting or infrared equipment may need to be installed in poorly lit areas;

• Cameras must be properly maintained and serviced to ensure that clear images are recorded and a log of all maintenance activities kept; and

• As far as practical, cameras must be protected from vandalism in order to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit within a vandal resistant casing.

Retention and Disposal

- CCTV images are not to be retained for longer than necessary, taking into account the purposes for which they are being processed. Data storage is automatically managed by the CCTV digital records which overwrite historical data in chronological order to produce an approximate 28-day rotation in data retention.
- Provided that there is no legitimate reason for retaining the CCTV images (such as for use in disciplinary and/or legal proceedings), the images will be erased following the expiration of the retention period.
- All retained CCTV images will be stored securely.

Third Party Access

Third party requests for access will usually only be considered in line with in the following categories:

• Legal representative of the Data Subject;

• Law enforcement agencies including the Police;

• Disclosure required by law or made in connection with legal proceedings; and

• HR staff responsible for employees and administrative staff responsible for students in disciplinary and complaints investigations and related proceedings.

- The Data Protection and Information Compliance team (Principal, Admin officer and safety officer) will disclose recorded images to law enforcement agencies including the Police once in possession of a form certifying that the images are required for either: an investigation concerning security; the prevention or detection of crime; or the apprehension or prosecution of offenders, and that the investigation would be prejudiced by failure to disclose the information.
- Where images are sought by other bodies/agencies with a statutory right to obtain information, evidence of that statutory authority will be sought before CCTV images are disclosed.
- Every disclosure of CCTV images is recorded in the CCTV Operating Log Book and contains:
  - The name of the police officer or other relevant person in the case of other agencies/bodies receiving the copy of the recording;
  - Brief details of the images captured by the CCTV to be used in evidence or for other purposes permitted by this policy;
  - The crime reference number where relevant; and
  - Date and time the images were handed over to the police or other body/ agency.
- Requests of for CCTV images for staff or student disciplinary purposes (or complaints purposes) must be authorised by HR or Principal/Admin Officer /Safety officer

Complaints Procedure

Any complaints relating to the CCTV system should be directed in writing to the safety officer/ admin officer promptly and in any event within 7 days of the date of the incident giving rise to the complaint. A complaint will be responded to within a month following the date of its receipt. Records of all complaints and any follow-up action will be maintained by the relevant office. If a complainant is not satisfied with the response they may appeal to the Principal. Complaints in relation to the release of images should be addressed to the Admin officer/ safety officer as soon as possible and in any event no later than one month from the event giving rise to the complaint.

Amendments:

Review 1	No Changes
Review 2	No Changes

Principal Mr. Paramjit Ahluwalia