Surveillance Devices Policy

1. Introduction

IQRA College has an obligation to ensure the safety and security of the School's environment by fulfilling their duty of care to students, staff, and visitors.

The visual presence of surveillance cameras strengthens the School's security, provides a strong deterrence against inappropriate behaviour, and often gives students a sense of security within the School's premises, while ensuring the privacy of individuals is protected in accordance with the *Surveillance Devices Act 2016* (SA), the APPs, the *Privacy Act 1988* (Cth) and IQRA College's Privacy Policy.

2. Scope

This Policy applies to the installation of surveillance cameras on IQRA College grounds and the use and disclosure of any footage produced by those cameras.

3. Purpose

Surveillance systems exist in and around the school to:

- Assist the School in fulfilling its obligations;
- Prevent and verify incidents, including but not limited to:
    - Illegal, unethical behaviour or misconduct of anyone on the School grounds
    - Other inappropriate behaviour, including of students, staff, visitors, or members of the public. *The school may use CCTV footage of incidents to help inform decisions about student management*
- Verify other incidents that may involve students, staff, and visitors;
- Provide enhanced capabilities to protect IQRA College, its facilities and assets against vandalism and theft; and
- Provide the principal with visual coverage

4. Access, Use and Disclosure

Surveillance cameras at IQRA College are NOT hidden or covert, located in private areas such as

toilets, changing rooms or staff rooms. They are installed in and around public areas of the School like entrance and exits, school yards, canteen, and corridors as part of their security systems and safety procedures.

Access to surveillance footage is strictly limited to the Principal, authorised personnel as determined by the Principal and the Leadership Team, and to those permitted by law.

Personal information accessed by authorised personnel will only be used and/or disclosed for the primary or secondary purpose for which it was collected, unless required by law or they have reason to suspect that an unlawful activity or serious misconduct that relates to the School's functions or activities has been, is being, or may be engaged in, and the School reasonably believes that the use or disclosure is 'reasonably necessary' in order to take appropriate action in relation to the matter.

Note: only the part of the camera footage that is directly relevant to the purpose will be used and disclosed. The principal will maintain an accurate Disclosure Register every time a disclosure has been made.

5. Safeguard Against Misuse of Personal Information

Surveillance footages are handled in strict accordance with the provisions of the privacy Act, particularly with regard to the APPs set out therein (including by having in place procedures, practices and systems that appropriately deal with the collection, use and disclosure of such information as required by the Privacy Act).

Personal information obtained from a surveillance footage will be adequately protected against misuse, loss and unauthorised access, or unlawful use and disclosure through adopting physical, technical, and operational safeguards.

Physical safeguards may include but not limited to:

- Suitable storage for digital records;
- Placing cameras out of reach and in secure casing;

- Using locks for access to control rooms and data storage areas; and

Technical safeguards may include but not limited to:

- Using password protection to restrict access to stored footage;
- Transmitting and storing footage in encrypted form;
- Encrypting any footage stored on portable storage devices; and
- Deleting or writing over footage that is no longer required.

Operational safeguards may include but not limited to:

- Limiting the number of staff who can access footage;
- Maintaining an audit trail of who accesses footage and when it is accessed; and
- Establishing clear protocols for responding to requests for access to, or copies of, footage (for example, determining who has authority to release footage, and how copies of footage are to be distributed).

6. Management of CCTV Cameras

The principal and the IT management team have the responsibility for the ongoing management of the CCTV systems installed around the school. IT staff will regularly check and confirm the operation of the system to ensure that it complies with relevant laws and procedures and this Policy.

Live CCTV footage will be displayed on the TV in the principal's office, allowing the principal to monitor school operations in real time effectively. The system includes a speaker function that enables the principal to communicate directly through the CCTV at any time, facilitating prompt interactions as needed. Access to sound recordings, however, will be strictly reserved for the principal or the discipline coordinator in situations requiring an investigation.

An annual review will be undertaken by IT staff in conjunction with the School Leadership Team to ensure existing surveillance cameras are situated in appropriate locations and are maintained and upgraded when required.

7. Storage and Deletion of Footage

The period in which a footage will be retained depends on the type of footage recorded, the reason the footage was originally created; and whether or not the footage provides evidence of an incident, crime or other information and/or evidence of a particular activity.

If a surveillance footage contains evidence relied upon in a decision to suspend or expel a student, it must be retained for the same period of time the suspension/expulsion documents are required to be retained. This is because the footage relied upon will form part of the decision to suspend or exclude the student. Similarly, if a surveillance footage is used to capture a workplace accident or personal injury giving rise to a personal injury or Work Cover claim, the footage must be retained for as long as the claim documents must be retained.

Continuous surveillance footage that is not required as evidence or requested by investigative and law enforcement agencies will be retained for a minimum period of 90 days. If no request has been made to view or access footage during this period, the footage will be deleted.