

# CCTV Surveillance Policy

## Policy Rationale

---

Imagine Education Group Pty Ltd (and each of its related entities) (“Imagine”) operates Closed Circuit Television Systems (CCTV) in various internal and external locations throughout the property.

The aim of this policy is to clearly outline the purpose of, use of and access to CCTV recordings by the company. Our CCTV cameras will give parents, staff and the wider community an increased sense of security.

## Policy Overview

---

### Definitions

The following definitions are used in this Policy:

**CCTV** means closed circuit television and similar surveillance equipment.

**Surveillance Controller** means the designated senior executive or manager employed by Imagine with overall accountability for CCTV.

**Authorised Person(s)** means any manager, employee or contractor authorised by Imagine to deal with operational and usage matters regarding CCTV in accordance with this Policy.

**Personal Information** means any information that allows an Individual to be identified. Images recorded using CCTV fall within this definition.

**Individual** means any individual who has his or her Personal Information collected, held and used by Imagine and/or Authorised Person(s).

**Surveillance Legislation** means the Telecommunications Interception Act 2009 (QLD) and the Privacy Act 1988 (Cth) and includes any directions, regulations, codes of practice and principles under these Acts.

### Purpose

Imagine operates CCTV systems for the purposes of:

- Prevention, deterrence and notification of break-ins or attempted break-ins, crime, theft and vandalism;
- Monitoring the security of Imagine premises;
- Ability to investigate and report on incidents where surveillance provides supporting evidence;
- Providing assurance, security and safety to employees, children, visitors, volunteers, contractors, and members of the public entering the centre; and

- Educator training.

Recorded images are retained and used only in accordance with the purpose for which the CCTV system was installed unless they are subject to State or Federal laws that may require these records to be used as evidence in legal proceedings or otherwise in accordance with the provisions of this policy.

## **Installation and Maintenance**

Imagine is responsible for ensuring that CCTV installation and use is compliant with relevant Commonwealth, State and Territory and Local Government laws and regulations at all times. Imagine and its Surveillance Controller will ensure that:

- Imagine engages the services of qualified, licensed and reputable third-party contractors to install its CCTV systems;
- Cameras are only installed in accordance with relevant Commonwealth, State and Territory laws;
- CCTV cameras and storing devices are well maintained and checked for operational use on a regular basis as per manufacturer instructions; and
- CCTV cameras are clearly visible and not concealed in any way.

## **Communication of CCTV Presence**

Imagine will ensure that reasonable steps are taken to notify those entering and using each Imagine centre of the use of CCTV, this includes:

- Access to the Imagine CCTV Surveillance Policy upon child enrolment;
- Notifying employees upon employment;
- Erecting clearly visible signage at the entrance of the centre to notify staff, families and visitors about surveillance; and
- Ensuring that cameras are in clear view and not hidden in any way.

## **Location of Cameras for Use**

Imagine will ensure that the location of any CCTV camera is such to maintain the dignity of those at the service and provide coverage to meet the purpose of the system. Cameras are to be directed at areas rather than individuals.

Specific camera locations will vary from centre to centre. However, in any given centre a clearly visible camera may be present in the following locations:

- Carpark and external walls;
- Entry and reception areas;
- Hallways;
- Kitchens;
- Studios and Playrooms; and
- Outdoor play spaces.

Cameras will not be placed in or be able to reach any of the following locations:

- Toilets;
- Change rooms;
- Bathrooms and showers;
- Breastfeeding locations;
- Areas put aside for prayer;
- Staff rooms;
- Storerooms; and
- Laundries.

The CCTV systems that Imagine use do not record sound.

The planning and design of each system has endeavoured to ensure that they will provide maximum effectiveness and efficiency within the confines of the law, however it is not possible to guarantee that any system will cover or detect every single event which takes place in the centre or within the areas of coverage.

Imagine will regularly review the systems to ensure that they are functioning correctly, whether additional cameras are necessary and that the existing cameras are situated in the most appropriate locations (and installed to maximise coverage). Imagine also reserves the right to remove any one or more cameras at any given centre at its discretion.

### **Retention of CCTV Data**

The Surveillance Legislation does not prescribe any specific minimum or maximum retention periods which apply to all CCTV systems or footage. Rather, the Surveillance Legislation requires that records containing Personal Information be destroyed or permanently de-identified when no longer needed for any purpose for which the information may be used or disclosed under the Surveillance Legislation.

This means that a balance must be struck between retaining CCTV footage in accordance with applicable retention periods and destroying them when they are no longer required for any legitimate business purpose.

Imagine does not keep images or video for longer than strictly necessary to meet its own purposes for recording them (this period has been generally treated as 30 days).

On occasion, Imagine may need to retain images for a longer period, for example where a law enforcement body are investigating a crime or incident, to afford them opportunity to view the images as part of an active investigation. For example, usually Imagine would only need to retain images for a short period of time because incidents will come to light very quickly. However, if a crime has been reported to the police, the images or video should be retained until the police have collected them.

## **Storage of CCTV Data**

The imagery recording systems (recorders and storage devices) which Imagine uses as part of its CCTV system are kept in lockable enclosures to protect against unauthorised access or vandalism.

The CCTV monitoring devices will be located in secure locations where they are unlikely to suffer from criminal attack or unauthorised access. Computers able to access images are password protected. Access is only provided to the Surveillance Controller and/or the Authorised Person.

Given the large amount of data generated by surveillance systems, Imagine may store video footage using a cloud computing system. We will take all reasonable steps to ensure that any cloud service provider maintains the security of our information, in accordance with industry standards.

We may engage data processors to process data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

## **Use of CCTV Data**

The CCTV recording system operates in real mode, monitoring the centre continuously 24 hours a day, 7 days a week throughout each year.

Imagine may rely on CCTV recordings to investigate alleged breaches of Imagine policies, laws, regulations and standards. Any such investigation will be carried out in accordance with the principles of natural justice and procedural fairness.

Where an incident has occurred or an allegation is made, the Surveillance Controller and/or an Authorised Person may review recorded CCTV to find out what happened and who was involved. This may include views before, during and after the incident with enough detail to recognise those present, and what happened including events leading up to and immediately after the event.

All requests to view, access or have released any CCTV recording must be immediately referred to the Surveillance Controller for consideration. Imagine will respond within a reasonable timeframe to any request. Disclosure of the recorded images to third parties can only be made in limited and prescribed circumstances in accordance with the Surveillance Legislation and Privacy Policy.

All requests for access or for disclosure must be recorded. If access or disclosure is denied then the reason is also documented. If access to or disclosure of the images is allowed, the following must also be documented:

- (a) The date and time at which access was allowed or the date on which disclosure was made.
- (b) The identification of any third party allowed access or to whom disclosure was made.
- (c) The reason for allowing access or disclosure.

- (d) The extent of the information to which access was allowed or which was disclosed.

## Data sharing & security measures

There will be occasions when Imagine needs to share its data with a third party (for example, providing CCTV footage to law enforcement bodies), and in doing so Imagine must comply with the Surveillance Legislation.

Imagine are required to deal with Personal Information in accordance with the Surveillance Legislation and to take appropriate technical and organisational measures to protect the Personal Information we processes. This applies whether we process it ourselves or if someone else (such as a contractor or service provider) does it for us.

Third parties which are provided with Personal Information by Imagine, must only:

- process, use and disclose the Personal Information in line with our instructions and the provisions of the Surveillance Legislation; and
- take appropriate security measures to retain confidentiality and protect the data. This includes the use of appropriately trained staff and the provision of secure storage for the data.

The method of disclosing images must be secure to ensure they are only seen by the intended recipient. It is for the Surveillance Controller to decide the most appropriate method to achieve this and the following options should be considered:

- Personal exchange.
- Courier delivery.
- Recorded delivery.
- Electronic transfer using encryption/password protection.

## Access by Individuals

Individuals have a right of access to their Personal Information. All Authorised Person(s) are to be trained to recognise a request for access to Personal Information by Individuals. All Individuals access requests are to be co-ordinated by the Surveillance Controller or his/her representative.

Individuals requesting access to their Personal Information are to be provided with a copy of this Policy and our Privacy Policy, which explains the purpose(s) for which images are recorded and retained and information about the disclosure policy in relation to those images.

The Surveillance Controller must also determine whether such images may be disclosed in accordance with the Surveillance Legislation or if an exception applies. If third party images are to be disclosed then the Surveillance Controller will arrange, where possible and if paid for by the Individual making the request, for the third party images to be disguised or blurred. If the Surveillance Controller decides that a subject access request is not to be complied with then the following must be documented:

- The identity of the Individual making the request.

- The date of the request.
- The reason for refusing to supply the images requested.

### Further Information

Please contact the Surveillance Controller at 07 5585 4901 for further information or questions regarding this CCTV Surveillance Policy.

### Policy Reference Information

---

**Education and Care Services Regulations: 261, 263**  
**Link to National Quality Standard: Elements 2.1.1, 2.2.1, 3.1.1 and 7.1.2.**

#### Related Forms:

#### Related Policies:

Privacy Online Policy

#### Reviewed:

This policy was **reviewed 14<sup>th</sup> May 2021**

This policy is due to be **re-reviewed 1<sup>st</sup> July 2021**

#### Sourced:

Holding Redlich Legal Expert Professionals

**This information was sourced on the 14<sup>th</sup> May 2021**