

Empowering Preschools with Easy Video Privacy Compliance

Safeguarding & CCTV Redaction Starter Kit



Protecting privacy, empowering educators, and making video compliance effortless for every school.

In today's schools, video surveillance plays a vital role in ensuring the safety and security of students, staff, and visitors. At the same time, schools have a legal and ethical responsibility to protect the privacy of everyone captured on camera. This guide provides preschools, schools and higher education with a comprehensive framework to manage video data responsibly and in full compliance with Personal Data Protection Act PDPA and other safeguarding regulations.

Inside, you will find:

- Standard Operating Procedure (SOP): Clear, step-by-step instructions for handling video footage.
- Face-Blur Policy: Guidelines to ensure the identities of students, staff, and visitors are protected.
- Parental Request Templates: Ready-to-use forms to handle Personal Data Protection Act (PDPA) requests efficiently.
- Hallway Signage: Professional signs to communicate video monitoring and privacy practices across campus.

This guide is designed to help school administrators, IT and security personnel, and safeguarding officers implement video privacy practices that are practical, compliant, and easy to follow, ensuring that safety and privacy go hand in hand.

3	Section 1: Incident Video Redaction Standard Operating Procedure (SOP)
9	Section 2: Parent request handling template
14	Section 3: Visitor and Pupil Face-Blur Policy (Video Privacy Protection)
20	Section 4: Example signage for school hallways and around campuses.



Section 1

Incident Video Redaction Standard Operating Procedure (SOP)

**For Safeguarding and Security Teams — Preschools and
Schools**

1. Introduction

This Standard Operating Procedure (SOP) outlines the steps for securely redacting and managing video footage related to incidents that occur within preschool and school environments.

The purpose of this SOP is to:

- Protect the privacy of children, parents, and staff,
- Ensure compliance with Singapore's Personal Data Protection Act (PDPA), and
- Provide clear operational guidance for safeguarding and administrative teams when managing incident-related video footage.
- This SOP supports a privacy-first approach to handling personal data captured through surveillance systems in both preschool and school settings.

2. Scope

This SOP applies to all safeguarding, security, and administrative staff responsible for handling video footage recorded by the school's surveillance systems, including footage managed through redaction tools along with video management systems (VMS). All personal data that can identify a child, parent, visitor, or staff member within video recordings.

3. Regulatory References

This SOP aligns with the following regulations and guidelines:

1. **Personal Data Protection Act 2012 (PDPA, Singapore):** Governs how personal data—including identifiable video images—must be collected, used, stored, and disclosed. Schools and preschools must ensure that footage is used only for legitimate safety, security, or operational purposes.
2. **Early Childhood Development Agency (ECDA) Data Protection Guidelines:** Sets out specific privacy and confidentiality expectations for preschools handling children's data, including the collection and disclosure of CCTV footage.
3. **Ministry of Education (MOE) Data Management and Security Guidelines:** Defines how student-related data, including video records, should be protected and managed in primary and secondary schools.
4. **School or Centre Data Governance Policy:** Each institution's internal data protection framework for handling personal data and video recordings in compliance with PDPA and relevant agency requirements.
5. **International References (if applicable):** FERPA (U.S. Family Educational Rights and Privacy Act) and COPPA (Children's Online Privacy Protection Act), for international schools following dual compliance standards.

4. Definitions

1. **Redaction:** The process of obscuring or anonymizing identifiable information (e.g., faces, badges, license plates) from video footage.
2. **Incident Footage:** Video recordings captured around the time or location of an event involving students, staff, or visitors.
3. **Safeguarding Team:** Designated personnel responsible for reviewing and responding to incidents involving student safety and welfare.
4. **Authorized Reviewer:** Staff member with explicit permission to access unredacted footage for investigative purposes.
5. **Personal Data:** Any data, including video, that can identify an individual directly or indirectly, as defined by the PDPA

5. Roles and Responsibilities

Role	Responsibility
Centre Leader / Principal	Approves redaction requests and ensures PDPA compliance
Safeguarding or Operations Manager	Oversees redaction requests, assigns access levels, and ensures compliance.
System Administrator	Manages access control within the VMS and redaction software.
Designated Reviewer	Reviews incident footage, applies redactions, and verifies accuracy.
Data Protection Officer	Monitors PDPA compliance and reviews disclosure decisions
Legal/Compliance Officer	Approves release of redacted footage to third parties and maintains records.

6. Procedure

6.1 Request and Authorization

1. All video redaction requests must be submitted via a Video Access Request Form (digital or paper)
2. Requests should include:
 - Date, time, and location of the incident
 - Purpose of access (e.g., investigation, parent inquiry)
 - Name and role of the authorized requester
3. The Safeguarding Manager must approve access before footage is retrieved.

6.2 Footage Retrieval

1. Access footage from authorized VMS system.
2. Access only the segments relevant to the incident — avoid unnecessary data collection.
3. Do not export or share footage before redaction.

6.3 Redaction Process

1. Open footage in approved redaction software.
2. Apply automated redaction to blur identifiable individuals not involved in the incident.
3. Use manual redaction tools for areas the AI does not automatically detect (e.g., reflective surfaces, screens, or background faces)
4. Verify the redacted video to ensure all identifiable data is properly obscured.
5. Export the redacted version using school-approved formats (e.g., MP4, AVI)

6.4 Access Duration and Retention

1. Authorized users may access unredacted footage for a maximum of 7 calendar days, unless legally required for longer retention.
2. Redacted copies must be securely stored for 90 days or according to internal retention policy.

3. Unredacted versions must be deleted once the redacted version has been verified and approved by the DPO or Principal.

6.5 Sharing and Disclosure

1. Only redacted footage may be shared with:
 - Parents or guardians (upon approved request)
 - Law enforcement authorities
 - Legal representatives or regulators (if required)
2. All disclosures must be approved by the DPO or Centre Leader and recorded in the Disclosure Log, which must include:
 - Date and purpose of disclosure
 - Recipient's name and organization
 - Authorization details

7. Security and Compliance

1. Store all footage on encrypted school servers or PDPA-compliant cloud environments located in Singapore.
2. Maintain detailed audit logs of all footage accessed, redacted, or shared.
3. All staff with access to CCTV or video redaction tools must complete annual PDPA and privacy awareness training.
4. Password-protect all video systems and apply two-factor authentication where possible.
5. Restrict video access strictly to authorized personnel only.

8. Incident Review and Continuous Improvement

1. Conduct quarterly reviews of video redaction and access practices to ensure ongoing PDPA compliance.
2. Report any data breaches, accidental exposure, or unauthorized access to the Personal Data Protection Commission (PDPC) within the legally required timeframe.

3. Review and update this SOP annually, or sooner if new MOE, ECDA, or PDPC guidelines are released.

Document Information:

Document Owner: Safeguarding & Compliance Team

Version: 1.0

Effective Date: [Insert Date]

Review Date: [Insert Date]

Section 2

Parent Request Handling Template

For Safeguarding and Security Teams — Preschools and Schools

1. Introduction

This form is used by parents or guardians to request access to CCTV footage related to an incident involving their child within school or preschool premises.

All requests will be handled in accordance with the Personal Data Protection Act (PDPA) and the school's Incident Video Redaction Standard Operating Procedure (SOP). To protect the privacy of all individuals, only redacted footage may be shared externally.

2. Parent / Guardian Information

Full Name: _____

Relationship to Student:

☐ Parent ☐ Legal Guardian ☐ Other: _____

NRIC/FIN (last 4 characters only) _____

Phone Number: _____

Email Address: _____

Mailing Address: _____

3. Student Information

Student Full Name: _____

Date of Birth: _____

Grade/Class: _____

School Name: _____

4. Details of the Request

Date of Incident: _____

Approximate Time: _____

Location (e.g., classroom, playground, corridor): _____

Brief Description of the Incident or Reason for Request:

Purpose of Request:

☐ To understand incident ☐ For insurance legal claim

☐ Other (Please specify) _____

Type of Access Requested:

☐ View Footage (in person) ☐ Receive Redacted Copy (if permissible)

5. Privacy & Access Policy

1. Access will be granted only if your child is the sole identifiable student in the footage, or if other individuals can be redacted to protect their privacy.
2. Requests that involve other identifiable students or ongoing investigations may be denied or delayed.
3. The school district will ensure all footage shared complies with FERPA, FOIA, and internal safeguarding policies.

6. Acknowledgement and Consent

Please read and acknowledge the following before submission:

- ☐ I understand that the school will only release **redacted footage**, where other children, staff, or visitors are not identifiable.
- ☐ I acknowledge that all CCTV footage is the property of the school and is managed under the **Personal Data Protection Act (PDPA)**.
- ☐ I consent to the school using the information provided in this form to process my request and to contact me regarding the outcome.
- ☐ I understand that the school reserves the right to refuse disclosure if the request conflicts with privacy regulations or internal safeguarding policies.

Signature: of Parent/Guardian _____

Date: _____

7. For School Use Only

Step	Description	Details
1	Date Request Received	
2	Received By (Name & Position)	
3	Request Reference Number	
4	Approved By (Principal / Centre Leader / DPO)	☐ Approved. ☐ Rejected
5	Date of Review	
6	Reason for Rejection (if applicable)	
7	Notes on Footage Retrieved	
8	Redaction Completed By	
9	Date of Redacted Footage Release	
10	Released To	
11	Method of Delivery	☐ Secure Download ☐ In-person Viewing ☐ Other: _____
12	Staff Signature	
13	Remarks	

8. PDPA Compliance Notice (To Be Retained Internally)

All requests and disclosures must comply with:

- Personal Data Protection Act (PDPA 2012)
- ECDA / MOE Data Management Guidelines
- The school's internal Video Redaction and Data Protection SOP

Redacted copies of footage shall be retained for **90 days** or as per the school's retention policy. Unredacted versions must not be disclosed externally.

9. Internal Notes (Confidential)

10. School Contact for Data Protection Enquiries

For questions regarding your request or data handling policies, please contact:

Data Protection Officer (DPO):

Name: _____

Email: _____

Phone: _____

Document Information:

Document Owner: Safeguarding & Compliance Team

Version: 1.0

Effective Date: [Insert Date]

Review Date: [Insert Date]

Section 3

Visitor and Pupil Face-Blur Policy (Video Privacy Protection)

In accordance with PDPA Safeguarding
Regulations

1. Introduction

The purpose of this policy is to outline how the school protects the privacy of pupils, parents, staff, and visitors captured on video surveillance systems.

This includes the automatic or manual blurring (redaction) of identifiable faces and personal information before footage is viewed, shared, or released outside the school.

The goals are to:

1. Safeguard the privacy and safety of all individuals on school premises.
2. Comply with Singapore's Personal Data Protection Act (PDPA 2012) and related regulatory guidelines.
3. Ensure responsible and transparent handling of CCTV and incident video footage.

2. Scope

This policy applies to:

1. All video footage recorded within school or preschool property, including CCTV, classroom cameras, and authorized body-worn or mobile devices.
2. All school personnel who access, review, process, redact, or share video footage.
3. External requests for video footage made by parents, guardians, or regulatory authorities under lawful grounds.

3. Legal & Regulatory Framework

This policy is governed by:

1. Personal Data Protection Act 2012 (PDPA) – governing the collection, use, and disclosure of personal data.
2. Ministry of Education (MOE) and Early Childhood Development Agency (ECDA) Data Protection and Security Guidelines.
3. Public Sector (Governance) Act and Instruction Manuals on Data Management (for government-affiliated preschools).
4. School or Operator Data Protection Policy and internal Data Retention Procedures.

Under the PDPA and related regulations:

1. Any video footage where an individual (child, parent, or staff) can be identified constitutes personal data.
2. Disclosure or use of such footage must have valid consent or fall within permitted exceptions under the PDPA (e.g., investigations, emergencies, or legal obligations).

4. Policy Statement

The school is committed to protecting the personal data of all individuals captured on video systems.
To ensure privacy and compliance:

1. Faces of non-consenting individuals will be blurred before footage is viewed, shared, or disclosed externally.
2. Any identifiable data (e.g., name badges, license plates, or sensitive displays) will be masked or redacted.
3. Only authorized staff trained in video handling and PDPA compliance may process or share such footage.
4. All redaction activity will be recorded in a Video Redaction Log for audit and accountability purposes.

5. Redaction Responsibilities

Role	Responsibility
Data Protection Officer (DPO)	Oversees compliance with PDPA and approves video release.
Safeguarding/Operations Manager	Reviews and approves internal requests for footage.
IT / Security Administrator	Retrieves footage and ensures it is securely stored and processed
Redaction Specialist / Administrator	Applies facial and object redaction using approved software
Principal / Centre Leader	Provides final authorization before footage is released.

6. When Face-Blur is Required

Face-blur (video redaction) must be applied when:

1. A parent or guardian requests access to footage that includes other children or staff.
2. Footage is shared with external authorities (e.g., ECDA, Police, insurance providers).
3. Footage is used for staff training, safety briefings, or school communications.
4. Any part of the video will be shown externally (e.g., to contractors, maintenance teams, or third parties).

Any video is released externally beyond the school's authorized personnel.

7. Redaction Standards

All redaction (blurring or masking) must:

1. Completely obscure identifiable faces, names, or sensitive visuals.
2. Be irreversible and permanent before the footage is shared externally.
3. Be logged, time-stamped, and verified by an authorized reviewer.
4. Be performed only with school-approved software such as (Facit Identity Cloak) or equivalent tools.

8. Data Storage & Retention

1. Original (unredacted) footage will be stored securely for no longer than 30 days, unless related to an ongoing investigation or disciplinary process.
2. Redacted copies released for legitimate requests will be stored securely for 90 days for auditing purposes.
3. All video files must be stored in encrypted servers or secure cloud environments approved by the school's IT department.
4. Access to unredacted footage is restricted strictly to authorized personnel.

9. Training & Awareness

All staff who handle or access CCTV footage must undergo annual PDPA and video privacy training, which includes:

1. Data protection and consent management under PDPA.
2. Safe handling, storage, and sharing of personal data in video form.
3. Proper use of redaction software to protect identities.

10. Breach Management

If unredacted or identifiable footage is disclosed without authorization:

1. The incident must be reported immediately to the School Data Protection Officer (DPO) and the Principal/Centre Leader.
2. The breach must be recorded in the Data Breach Log and investigated in line with the school's Data Breach Response Plan.
3. The DPO will assess whether the incident is notifiable to the Personal Data Protection Commission (PDPC) under the PDPA.

11. Review and Audit

This policy will be:

1. Reviewed annually or earlier if regulatory requirements change.
2. Audited periodically to ensure that redaction and video-handling practices remain compliant and effective.
3. Updated whenever new surveillance technologies or privacy risks are introduced.

12. References

1. Personal Data Protection Act 2012 (Singapore)
2. PDPC Advisory Guidelines for Education Institutions
3. Ministry of Education (MOE) Data Management & IT Security Guidelines
4. Early Childhood Development Agency (ECDA) Data Protection Policy
5. School's Internal Data Retention and Privacy Framework

Document Information:

Policy Owner: Safeguarding & Compliance Department

Approved By:

Version: 1.0

Effective Date of Approval: [Insert Date]

Next Review Date: [Insert Date]

Section 4

Example Signage for School and Preschool campuses (Privacy & Video Surveillance)

To comply with with Singapore's Personal Data
Protection Act (PDPA)

1. Introduction

To support the school's **Video Redaction and Face-Blur Policy**, clearly visible signage should be displayed throughout school and preschool premises.

These signs serve to:

1. Inform pupils, staff, parents, and visitors that video surveillance (CCTV) is in operation on the premises.
2. Communicate that video recordings may be subject to blurring or redaction of identifiable faces and personal information, in line with privacy and safeguarding requirements.
3. Reinforce the school's commitment to protecting personal data under Singapore's Personal Data Protection Act (PDPA 2012) and relevant MOE/ECDA data protection guidelines.

Sign Option 1 – General Surveillance Notice (for Entrances & Common Areas)

Video Surveillance in Operation

- This school/preschool uses CCTV cameras for the safety and security of our pupils, staff, and visitors.
- Video recordings may be used for safety investigations and may be subject to privacy redaction (e.g., face blurring) before review or sharing.
- All video data is handled in accordance with the **Personal Data Protection Act (PDPA)** and the school's **Data Protection Policy**

For enquiries, please contact:
Data Protection Officer (DPO)
[Insert School Name]
[Insert DPO Email / Contact Number]

Sign Option 2 – Classroom or Indoor Learning Area Signage

CCTV IN USE FOR SAFETY AND LEARNING

- This area is monitored by CCTV to maintain a safe environment for pupils and staff.
- Any identifiable footage will be securely managed and may be blurred or anonymised when shared.
- For questions about how personal data is used, please contact our **Data Protection Officer (DPO)**

Sign Option 3 – Office or Reception Area Signage (For Visitors & Parents)

YOUR PRIVACY MATTERS

- Video recording is in operation within the school for safety and operational reasons.
- The school complies with the **Personal Data Protection Act (PDPA)** and takes steps to protect the identities of children, parents, and staff in any footage shared.
- You may contact the **Data Protection Officer (DPO)** for more information on our privacy and CCTV policies

Sign Option 4 – Preschool Playground or Outdoor Area Signage

KEEPING OUR CHILDREN SAFE

- CCTV monitoring is in place in this area to ensure the well-being of pupils and staff.
- Video may be reviewed for safety purposes and redacted (faces blurred) where required to protect privacy.
- For more details, please contact the **Centre Leader** or **Data Protection Officer (DPO)**.

Sign Option 5 – Visual + Text for Younger Students

Smile! You're on Camera

- For safety, we have cameras here.
- **Faces may be blurred** if videos are shared outside school.
- We protect everyone's privacy!

**Streamline the redaction process,
reduce the risk of privacy breaches and
ensure ongoing support in safeguarding
student privacy. Email info@facit.ai to
find out more. Or visit [Facit.ai](https://facit.ai)**

