Facit

Empowering K-12 Schools with Easy Video Privacy Compliance

Safeguarding & CCTV Redaction Starter Kit

Facit

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 K–12 schools with a comprehensive framework to manage video data responsibly and in full compliance with FERPA, FOIA, and state safeguarding regulations.

Inside, you will find:

- **Standard Operating Procedure (SOP):** Clear, step-by-step instructions for hand 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 FERPA and FOIA 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)
8	Section 2: Parent request handling template
12	Section 3: Visitor and Pupil Face-Blur Policy (Video Privacy Protection)
17	Section 4: Example signage for school hallways and around campuses.

Facit

Section 1

Incident Video Redaction Standard Operating Procedure (SOP)

For Safeguarding and Security Teams — K-12 Schools

Facit

1. Introduction

This SOP outlines the procedures for securely redacting and managing video footage related to incidents within K-12 school environments. The goal is to protect student and staff privacy while maintaining compliance with federal and state privacy regulations.

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).

3. Regulatory References

This SOP aligns with the following regulations and guidelines:

1. **FERPA (Family Educational Rights and Privacy Act, 20 U.S.C. 1232g):** Governs access and disclosure of student education records, including identifiable video footage.
2. **COPPA (Children's Online Privacy Protection Act):** Protects children's data under 13 years of age.
3. **HIPAA (Health Insurance Portability and Accountability Act):** Applies if footage includes health-related contexts, such as nurse's offices or medical incidents.
4. **State-Specific Student Privacy Acts**: Follow state-level legislation such as California's Student Online Personal Information Protection Act (SOPIPA) and Texas Education Code 26.004.
5. **School District Data Governance Policy:** Each district's internal policy for managing student data and security recordings.
6. **Freedom of Information Act (FOIA, 5 U.S.C. 552):** Regulates public access to government-held records. In the context of public schools, it may apply to video footage requests; however, disclosures must comply with FERPA to prevent releasing personally identifiable information.

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. Roles and Responsibilities

Role	Responsibility
Safeguarding 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.
Legal/Compliance Officer	Approves release of redacted footage and ensures adherence to legal standards.

Facit

6. Procedure

6.1 Request and Authorization

1. All video redaction requests must be submitted via a Video Access Request Form (internal or digital system).
2. Requests should include:
    - Incident date, time, and location
    - Reason for request
    - Authorized personnel requesting access
3. The Safeguarding Manager must approve access before footage is retrieved.

6.2 Footage Retrieval

1. Access footage from the approved Milestone XProtect or other authorized VMS system.
2. Retrieve only the segments relevant to the reported incident.
3. Do not export or share footage before redaction.

6.3 Redaction Process

1. Open footage in Facit Identity Cloak or approved redaction software.
2. Apply automated facial and object anonymization to obscure identifiable individuals not involved in the incident.
3. Use manual redaction tools for additional masking if automated detection misses certain areas.
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) with encryption enabled.

6.4 Access Duration and Retention

1. Authorized users can access unredacted footage for a maximum of 7 days unless extended by legal requirement.
2. Redacted copies should be stored securely for 90 days or per district policy.

3. Delete unredacted versions after approval and verification of the redacted file.

6.5 Sharing and Disclosure

1. Only redacted versions may be shared with external parties (parents, law enforcement, or legal representatives).
2. The Legal/Compliance Officer must authorize all external disclosures.
3. Maintain a log of all shared footage, including recipient details and date.

7. Security and Compliance

1. All footage must be stored in **encrypted school servers or approved cloud environments**.
2. Audit trails must be maintained for each video accessed or redacted.
3. Staff handling footage must complete **annual data protection training** per FERPA and local district requirements.

8. Incident Review and Continuous Improvement

1. Conduct quarterly reviews of redaction practices.
2. Report any data breaches or unauthorized disclosures to the District Compliance Office within 24 hours.
3. Update the SOP annually or as regulatory changes occur.

Document Information:

Document Owner: Safeguarding & Compliance Team
Version: 1.0
Effective Date: [Insert Date]
Review Date: [Insert Date]

Facit

Section 2

Parent Request Handling Template

For Safeguarding and Security Teams — K-12 Schools

Facit

1. Introduction

This form allows parents and legal guardians to request access to school video footage that may include their child.

All requests are processed in compliance with the Family Educational Rights and Privacy Act (FERPA), the Freedom of Information Act (FOIA), and the school district's Safeguarding and Privacy Policy.

2. Parent / Guardian Information

Full Name: _____

Relationship to Student:
☐ Parent ☐ Legal Guardian ☐ Other: _____

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., hallway, cafeteria, parking lot): _____

Brief Description of the Incident or Reason for Request:

Facit

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. Parent / Guardian Certification

I certify that I am the **parent or legal guardian** of the student named above.

I understand this request will be processed in line with applicable federal and district regulations.

Signature: _____

Date: _____

Facit

7. For School Use Only

Step	Description	Responsible Staff	Date	Status
1	Verify parent/guardian identity	Safeguarding Officer		☐ Complete
2	Locate relevant footage	IT / Security		☐ Complete
3	Assess presence of other individuals	Compliance Officer		☐ Complete
4	Redact footage if needed	Video Redaction Team		☐ Complete
5	Schedule viewing / share redacted copy	Admin		☐ Complete
6	Log request in FERPA records	Records Manager		☐ Complete

8. Internal Notes (Confidential)

Legal References

1. Family Educational Rights and Privacy Act (FERPA) — 20 U.S.C. 1232g
2. Freedom of Information Act (FOIA) — 5 U.S.C. 552
3. 34 CFR Part 99 — Education Records Access
4. Applicable State and District Privacy Regulations

Document Information:

Document Owner: Safeguarding & Compliance Team
Version: 1.0
Effective Date: [Insert Date]
Review Date: [Insert Date]

Facit

Section 3

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

In accordance with FERPA, FOIA, and School Safeguarding Regulations

Facit

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 reviewed, shared, or released outside the school.
The goal is to:

1. Safeguard pupil and visitor privacy,
2. Comply with **FERPA** and **FOIA** regulations, and
3. Ensure responsible handling of visual data in incident reviews or information requests.

2. Scope

This policy applies to:

1. All video footage recorded on school property (CCTV, security cameras, or authorized body-worn devices).
2. Any school personnel who access, review, process, redact, or share video footage.
3. External requests for video footage made under **FERPA**, **FOIA,** or school safeguarding protocols.

3. Legal & Regulatory Framework

This policy is governed by:

1. Family Educational Rights and Privacy Act (FERPA) – 20 U.S.C. 1232g
2. Freedom of Information Act (FOIA) – 5 U.S.C. 552
3. 34 CFR Part 99 – Protection of Education Records
4. State and District Privacy and Safeguarding Guidelines

Under these regulations:

1. Video footage that identifies a student is considered an **education record.**
2. Footage that identifies non-students (e.g., visitors) may be subject to **FOIA**, provided it does not compromise personal privacy.

Facit

4. Policy Statement

The school is committed to ensuring that all identifiable individuals captured on video — including **students, visitors, and staff** — are protected through video redaction and anonymization before footage is viewed or released.

The school will:

1. Blur or mask faces of all non-consenting individuals visible in any video footage before sharing it outside the school.
2. Ensure that pupil identities are protected in compliance with FERPA, unless a parent or guardian has provided written consent.
3. Use secure, school-approved redaction software to process footage.

Maintain a video redaction log for all instances where footage has been edited, shared, or released.

5. Redaction Responsibilities

Role	Responsibility
Safeguarding Officer	Approves all requests for video review or release.
IT / Security Team	Retrieves and secures the requested footage.
Redaction Specialist / Administrator	Performs face-blur redaction using approved software.
Compliance Officer	Verifies FERPA/FOIA compliance and logs redaction activity.
School Principal	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 footage under FERPA that

includes other students or staff.

2. A public information request under FOIA could identify individuals.
3. Footage is shared with law enforcement, insurers, or contractors.
4. Footage is used for staff training or public communication.

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

7. Redaction Standards

All redaction (blurring or masking) must:

1. Completely obscure identifiable facial features, license plates, or names on badges.
2. Be irreversible and permanent before sharing externally.
3. Be logged and time-stamped, with redaction notes recorded for auditing.

8. Data Storage & Retention

1. Original (unredacted) footage will be retained securely for no longer than 30 days, unless linked to an active investigation.
2. Redacted versions released for compliance or parental requests will be securely stored and logged for auditing.
3. Access to unredacted footage is restricted to authorized staff only.

9. Training & Awareness

All safeguarding officers, administrators, and technical staff involved in video handling must complete annual training on:

1. FERPA and FOIA privacy requirements,
2. Video redaction techniques, and
3. Secure storage and disclosure practices.

Facit

10. Breach Management

Any unauthorized disclosure of unredacted footage or identifiable personal data must be:

1. Reported immediately to the School Data Protection Officer (DPO) and Principal.
2. Logged and investigated as a privacy incident.
3. Remediated following the school's Data Breach Response Policy.

11. Review and Audit

This policy will be:

1. Reviewed annually, or sooner if regulations change.
2. Audited regularly to verify compliance and the effectiveness of redaction processes.

12. References

1. Family Educational Rights and Privacy Act (FERPA) – 20 U.S.C. 1232g
2. Freedom of Information Act (FOIA) – 5 U.S.C. 552
3. 34 CFR Part 99 – Student Privacy Regulations
4. U.S. Department of Education, Student Privacy Policy Office
5. Local State Safeguarding and Data Protection Legislation

Document Information:

Policy Owner: Safeguarding & Compliance Department
Approved By:
Version: 1.0
Effective Date of Approval: [Insert Date]
Next Review Date: [Insert Date]

Facit

Section 4

Example Signage for School Hallways and Around Campuses (Privacy & Video Surveillance)

To comply with FERPA, FOIA, and School Safeguarding Regulations

Facit

1. Introduction

To support the implementation of the Visitor and Pupil Face-Blur Policy, clearly visible signage should be placed throughout school premises. The signs serve to:

1. Inform students, staff, and visitors that **video surveillance is in operation**.
2. Communicate that **faces and other identifiable information may be blurred** in accordance with privacy, legal, and safeguarding requirements.
3. Reinforce awareness of the school's **commitment to FERPA, FOIA, and safeguarding compliance**.

The following signage options are designed to provide consistent, easily understandable guidance, ensuring that all individuals entering or moving within school areas are aware of privacy practices and expectations.

Sign Option 1 – General Awareness

Privacy Notice

- Video surveillance is active in this area.
- Faces of students, staff, and visitors may be blurred before any footage is reviewed or shared externally.
- This ensures compliance with **FERPA, FOIA, and School Safeguarding Regulations**.
- Thank you for respecting the privacy of our school community.

Facit

Sign Option 2 – Instructional / Reminder for Visitors

Notice to Visitors

- Cameras are in use for safety and security.
- **Faces may be automatically blurred** to protect privacy.
- All video handling follows strict **privacy and data protection rules**.
- By entering, you consent to surveillance under these privacy protocols.

Sign Option 3 – Staff / Internal Awareness

Video Privacy Compliance

- Video footage may contain identifiable individuals.
- Only **authorized staff** may access unredacted footage.
- **All external sharing requires face-blurring and approval.**
- Follow **FERPA, FOIA, and school safeguarding policies** at all times.

Facit

Sign Option 4 – Short and Eye-Catching (Hallway Posters)

Privacy in Action

- Cameras are recording.
- Faces of students & visitors **may be blurred** for privacy.
- Footage is handled according to **FERPA, FOIA, and school safeguarding rules**

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!

Facit

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