



Image Guidance for U.S. Schools

Protecting students and staff in the age of AI-generated imagery

A national edition for school districts, charter schools, independent schools, dioceses, BIE and Tribal schools, and state education agencies, with a state-law localisation layer.

1 The bottom line

Publish only what you would defend in a safeguarding review, a FERPA complaint, a Title IX investigation, and a state criminal referral, simultaneously.

IN PRACTICE

A small number of consented, low-identifiability images, captured on school-owned devices, stripped of metadata, downscaled, hosted on a channel the school controls, logged, reviewed every year, and deletable on request.

Why this matters now

- Any face published online is usable input for a "nudify", face-swap, or image-to-video model. The barrier is no longer skill or money, it is a free app and one clear photo of a child's face.
- Between January and September 2025, the NCMEC CyberTipline received more than one million reports relating to generative AI, and NCMEC recorded steep growth in online enticement and sextortion reporting. The Internet Watch Foundation recorded a 260-fold increase in AI-generated child sexual abuse videos in 2025.
- School websites, district and booster social feeds, athletics pages, livestream archives, and digital yearbooks are the highest-yield source of student images for offenders and sextortion rings: indexed by search engines, uniformed, rostered, name-tagged, dated, geolocatable, and almost never reviewed once posted.
- U.S. school cases are now documented and litigated, not hypothetical. Two students at a Pennsylvania independent school were sentenced in March 2026 over 347 explicit deepfake images and videos of 60 girls; a Louisiana middle-school case ended with the targeted 13-year-old girl herself expelled after the fallout. Both illustrate the same failure: no image-incident workflow, and a response that landed on the victim.
- The existing legal floor, FERPA, Title IX, COPPA, federal CSAM and obscenity law, the TAKE IT DOWN Act, the DEFIANCE Act, state mandatory-reporting duties, state NCII and deepfake statutes, and state student-privacy statutes, already requires this level of care. AI has raised the cost of getting it wrong, not the standard.

THE SINGLE SENTENCE TO GIVE YOUR BOARD

We cannot control what generative AI can do to an image. We can control how few images we expose, how identifiable they are, how quickly we can take them down, and how well we respond when something happens. This document governs all four.

2 Where this document sits

The United States has the criminal statutes, the privacy statutes, and the civil-rights framework. It does not have a national, image-specific operational layer for schools. Every district and school is expected to build that layer itself. This document supplies it, in a form that works in all fifty states, D.C., and the territories, with a localisation step for the parts that genuinely vary.

1. Federal education and privacy law

FERPA (20 U.S.C. 1232g and 34 CFR Part 99) governs whether a student photograph is an education record, whether it can be designated directory information, and what consent is required. The U.S. Department of Education has published dedicated FAQs on photos and videos under FERPA. COPPA (15 U.S.C. 6501–6506, as amended by the FTC's 2025 Rule amendments) governs third-party collection of images and identifiers from students under 13. Neither covers image capture practice, framing, metadata, channel choice, publication logs, or incident response.

2. Federal criminal and platform law

Federal CSAM and obscenity law, including 18 U.S.C. 2251, 2252A, and 1466A, reaches computer-generated and manipulated depictions. The TAKE IT DOWN Act creates a federal offence for knowingly publishing nonconsensual intimate visual depictions, including AI-generated ones, and requires covered platforms to provide a removal-request process and to remove a reported depiction, plus known identical copies, within 48 hours of a valid request. The FTC began enforcing that platform obligation on 19 May 2026. The DEFIANCE Act of 2024 gives victims a federal civil cause of action.

3. Federal civil rights

Title IX (34 CFR Part 106) applies where image manipulation is used as sex-based harassment between students, or by or against staff. As at September 2026, the 2020 Title IX regulations are the operative federal rule nationwide, following the January 2025 vacatur of the 2024 rule. Section 504 and the ADA apply where a student with a disability is targeted or where a photograph reveals disability status.

4. State law, the layer that actually bites

State law is where most schools get caught, and it is the only part of this document that must be localised. As at September 2026, research by ENOUGH ABUSE records 46 to 47 states with statutes criminalising AI-generated or computer-edited CSAM, and independent trackers record 48 states addressing sexually explicit deepfakes in some form, with more than 250 deepfake-related statutes nationwide. At least 40 states have student-data-privacy statutes that sit on top of FERPA. Every state makes school personnel mandated reporters, but the hotline, the timeframe, and the wording of the duty differ. Section 5 of this document is the worksheet for filling that in.

THE GAP THIS DOCUMENT FILLS

There is no federally issued document that answers the operational question: how should a school capture, select, publish, log, review, and respond to incidents involving student and staff images. This edition sits alongside federal law, state criminal and privacy statutes, and your state education agency's AI guidance, and supplies the operational layer those instruments assume but do not provide.

3 Situation and complication

Situation

Every school in the country captures student and staff images every week, assemblies, athletics and livestreamed games, band and drama, field trips, science fairs, state-testing celebrations, homecoming, prom, graduation, yearbook, enrolment marketing, grant reporting, and booster-club fundraising. Families expect to see these moments. Schools use them to celebrate, communicate, recruit, and fundraise. None of that is going to stop, and this document does not ask it to.

Complication

- Generative AI has made it trivial to strip clothing, swap faces, animate a still image, or fabricate sexual imagery from a single ordinary school photo, in seconds, on free consumer apps, from a phone, with no technical skill.
- Offenders lift student photos from school websites, athletics pages, and district social feeds, generate explicit material, and use it for sextortion against the student, the family, or the school.
- Once an image is public it cannot be recalled. It is copied, cached, mirrored, archived, indexed, and licensed onward by the platform under its own terms, including, on some platforms, for AI training.
- The most damaging cases are peer-to-peer, not stranger-danger. Students generate material about classmates, which makes this simultaneously a safeguarding matter, a Title IX matter, a discipline matter, a mandated-reporting matter, and a criminal matter.
- Consent given once at enrolment does not survive a technology change of this magnitude. Families increasingly expect granular, channel-specific, revocable, annually refreshed consent, and several state privacy statutes now push in the same direction.
- Athletics and livestreaming are the weakest link in most schools: third-party streaming platforms, booster-run accounts, rosters with names, heights, grade levels and jersey numbers, and archives nobody owns.

Question this document answers

How should a U.S. school or district capture, select, publish, log, review, and respond to incidents involving student and staff images, given generative-AI risk and the federal and state legal requirements that apply?

FERPA

A student photograph is not automatically directory information. Under FERPA it becomes directory information only if the school (a) has designated photographs as such in its annual notice to parents and eligible students, and (b) has given families a meaningful opportunity to opt out before disclosure.

If either step is missing, publishing an identifiable student photo without written consent is a FERPA problem, including on a routine district social media post. State privacy regulators have made determinations on exactly this point.

Even where designation is in place, coupling a photograph with any protected record, grade, class list, roster with academic detail, IEP or 504 status, disciplinary status, English-learner status, McKinney-Vento status, free-and-reduced-lunch status, immigration-adjacent detail, removes the exception and requires signed parent or eligible-student consent.

A student who has opted out of directory information must not appear in a public photo caption, alt text, filename, roster graphic, or tagged post. That requires an opt-out register the person holding the camera can actually check.

4 What is in this document

Section	What it gives you
1. Bottom line	The one-sentence rule to follow
2. Where this document sits	How this fits alongside federal law, state law, and state agency AI guidance
3. Situation and complication	Why the old approach is no longer safe
4. What is in this document	This table
5. Localise this document	The state-specific worksheet – complete this before adoption
6. Eight operating principles	The reasons behind the rule – memorise these
7. Before you take an image	Capture checklist, photographer brief, higher-care situations
8. Before you publish an image	Publishing test, selection, preparation, channel, log, review cycle
9. Athletics, livestreams, yearbooks	The four settings where schools lose control
10. Vendors and contracts	Clauses to insert, including AI-training prohibition
11. When something goes wrong	Incident workflow and national reporting lines
12. Federal legal and regulatory map	The federal instruments that apply
13. The state-law layer	What varies by state and how to check it
14. Roles and accountability	Who owns what

Section	What it gives you
15. Board-level assurance	Annual calendar and the six metrics to report
16. One-page checklist	Print, laminate, distribute
17. Family-facing summary	Paste into your newsletter or handbook
18. Model consent form	Channel-specific, revocable, annual
19. Sources and further reading	Every claim, with URLs

5 Localise this document to your state

This document is national. The fourteen items below are not. Complete the table below with district counsel before adoption, insert the answers into Sections 11, 12, and 13, and re-verify every twelve months, state legislatures have amended these statutes every session since 2023.

Field to complete	Where to find it	Your entry
1. State child-abuse reporting hotline and statutory timeframe	Your state child-welfare agency; Child Welfare Information Gateway state pages	
2. Exact mandated-reporter statute for school personnel	State code; your state education agency mandated-reporter training	
3. State NCII statute (nonconsensual intimate imagery)	State criminal code; state AG office	
4. State deepfake / synthetic intimate imagery statute	State criminal code; deepfake legislation trackers in Section 19	
5. State AI-generated or computer-edited CSAM statute	ENOUGH ABUSE state-law tracker; state criminal code	
6. State juvenile sexting provision and diversion pathway	State juvenile code; county prosecutor	
7. State student-records confidentiality statute (FERPA analogue)	State education code	

Field to complete	Where to find it	Your entry
8. State student-data-privacy statute (SOPIPA-style vendor duties)	Student Privacy Matters state chart	
9. Regional ICAC Task Force and its lead agency	icactaskforce.org (61 task forces nationwide)	
10. District attorney / county prosecutor contact	County prosecutor office	
11. State education agency AI and privacy guidance	State education agency website	
12. State youth crisis line, in addition to 988	State behavioral-health agency	
13. Address-confidentiality / safe-at-home program in your state	State Secretary of State or AG office	
14. Tribal jurisdiction, BIE, or diocesan reporting line where applicable	Tribal social services; BIE; diocesan safe-environment office	

DO NOT SKIP THIS SECTION

Federal law sets a floor. State law sets the ceiling, and it is state law that produces the prosecutor referral, the child-welfare investigation, the state privacy-office determination, and the parent complaint to your board. A document with blanks in this table is not yet a policy, it is a draft.

6 Eight operating principles

1. Consent must be informed, granular, revocable, and re-earned each year

Blanket "yes to all photos, forever" consent no longer meets community expectations, several state privacy statutes, or a defensible FERPA position. Split consent by channel, internal use, school website, public social media, external news media, yearbook, livestream, third-party platforms, refresh it annually alongside the annual FERPA notice, and honour withdrawal, including for images already published, to the extent removal is technically possible. Tell families honestly what you cannot undo.

2. The child's in-the-moment "no" outranks the parent's "yes"

A signed form is a permission, not a compulsion. A student who declines on the day must never be photographed, singled out, named to the group, moved out of shot conspicuously, or excluded from the activity itself. For eligible students, 18 or attending a postsecondary institution, FERPA rights have transferred and the student's own decision governs.

3. Capture on school-owned, school-managed devices only

Personal phones create untraceable copies, retain GPS and device metadata, sync automatically to personal cloud accounts, and expose staff to allegations they cannot disprove. Use only school-managed cameras or devices, with images landing in the school's Google Workspace for Education or Microsoft 365 tenant under role-based access and retention rules. If a member of staff has already captured something on a personal device, the rule is transfer to the tenant, then delete from the device, documented.

4. Reduce identifiability by default

Wider shots over close-ups. Activity over face. Side-on or over-the-shoulder where a close-up is unavoidable. No name adjacent to a face. Never combine uniform, mascot, school name, location marker, and student name in a single publishable asset. Blur, crop, or exclude where there is no educational purpose in identifying the child. Every element you remove is an element an offender cannot use.

5. Strip metadata and downscale before public publishing

Remove EXIF, IPTC, and XMP data, GPS, device, timestamp, author, serial number, and reduce resolution before any public post. High-resolution originals stay internal behind access control; low-resolution, metadata-stripped copies go public. Typically 1200 px on the long edge for web and less for thumbnails. Higher resolution is what makes a fabricated image convincing.

6. Publish on the least-public channel that achieves the purpose

Direct email, the learning management system, or the parent portal for class and cohort updates. The school website and public social media for genuine community-wide celebratory moments only. Ask what the purpose actually is: if the audience is forty families, do not publish to four billion people. Turn comments off on any public post carrying student images.

7. Staff and employee images are in scope too

Teachers, coaches, aides, and administrators are targeted with manipulated imagery by students, former students, and outsiders. Staff images require the same consent discipline, the same metadata hygiene, and the same incident workflow, plus employment-law and union considerations. Do not publish staff photographs alongside classroom locations, schedules, or personal contact details. Include staff explicitly in your policy scope and your incident register.

8. Every published image has an owner, a log entry, and a takedown date

An image with no named owner and no planned review date will sit online for a decade. Log every public publication, assign the channel to a named role, set a takedown or review date at the point of publication, and audit annually. This is the single control that most reduces long-run exposure, and it is the one most schools skip.

7 Before you take an image

Ask, in order:

- 1 Is there a defensible educational, communications, or statutory-reporting purpose that written work, a wide shot, a photo of the work rather than the child, or an anonymised alternative cannot serve?
- 2 Is current, informed, channel-specific consent on file for every student in the frame? Cross-check against the annual FERPA directory-information notice and the opt-out register.
- 3 Has anyone in the frame indicated, verbally or through body language, that they do not want to be photographed today?
- 4 Am I using a school-owned, school-managed device with secure storage in the school tenant?
- 5 Have I framed for activity, not identity, wide, side-on, or over-the-shoulder where possible?
- 6 Do I know how images of non-consenting students will be handled discreetly, without singling them out?
- 7 If this is a higher-care situation (see below), have I checked with the designated safeguarding or student-services lead first?

If a professional or contracted photographer is used

- Notify parents and students in advance and re-obtain channel-specific consent for that specific shoot. Enrolment consent is not shoot consent.
- Give the photographer a written brief: purpose, permitted uses, non-consent list, framing standards, storage handover to the school tenant, deletion timeline, and named school contact on the day.
- The contract must require the photographer to hand over all files, delete their own copies by a stated date, and not use images in their portfolio, marketing, competition entries, or stock libraries, and must prohibit use of the images as AI training data or submission to any AI service. See Section 10 for clause language.
- Agree a discreet method for identifying non-consenting students in advance, coloured wristbands, lanyard colour, a list held by the class teacher, never a public callout, never a separate room.
- A school staff member must be present and supervising for the whole shoot, including individual portraits.

Situations where extra care is required

In each of these cases the default is do not capture and do not publish unless the designated safeguarding or student-services lead has confirmed it is safe. The family never has to justify the request.

- Students in foster care, kinship care, or state child-welfare custody, or subject to any restricted-contact, custody, protective, or no-contact order.
- Students from families experiencing domestic violence or coercive control, or enrolled in a state address-confidentiality or safe-at-home program.
- Adopted students where the family has requested identity protection, and students in open-adoption arrangements with contact restrictions.
- Students with cultural, religious, or Tribal community reasons to avoid image capture, including students affiliated with federally recognised Tribes, and students in communities where photography of children is restricted.

- Students identified under McKinney-Vento as experiencing homelessness, in shelter accommodation, or in transitional housing.
- Students or families with immigration-status sensitivities, where a published image plus a location and time is a targeting risk.
- Students receiving special education services, where a photograph may reveal placement, service, or disability status, publishing that pairing requires written consent.
- Students who are subjects of, or witnesses in, a criminal, Title IX, or child-protection investigation.
- Students who have previously been targeted by image-based abuse, bullying, sextortion, or stalking.
- Students whose family has asked to minimise their online presence for any reason at all.

8 Before you publish an image

THE PUBLISHING TEST

If this image were downloaded, run through a nudify or image-to-video app, geolocated from the uniform and background, matched to a name from our own athletics roster, and re-posted with that name attached, would the school still be comfortable that it published this image, on this channel, at this resolution? If no, do not publish.

Selection

- Activity in focus, not the individual.
- Wide or group shot preferred; close-ups only where educationally necessary, and captured side-on.
- No safety or compliance concerns visible: unsafe practice, missing PPE, exposed lanyards with full names or student IDs, visible schedules, visible screens showing student data, visible medical equipment.
- No visible location markers combined with uniform, mascot, bus number, room number, or timetable clues.
- Clothing check: avoid images where ordinary activity, swimming, gymnastics, dance, athletics, dress-up days, water play, produces a frame that is trivially manipulable. This is not about modesty; it is about how these models work.
- No student in the frame who is on the opt-out register, in a higher-care category, or who declined on the day.

Preparation

- EXIF, IPTC, and XMP metadata stripped: GPS, device, timestamp, author, serial number, editing history.
- Resolution reduced to what the channel actually needs, typically 1200 px on the long edge for web, less for thumbnails.
- Filename anonymised, no student name, student ID, class code, teacher name, or date pattern.
- No student name in the caption, alt text, image title, or file metadata unless there is a specific consented reason. Write alt text that describes the activity, not the child.
- No cropping of a group photo down to a single child to "reuse" it, that changes the consent basis and the risk profile.
- Version control: the public copy is a separate, downscaled derivative. Never publish the original file.

Channel

- Least-public channel that serves the purpose. Prefer the parent portal, learning management system, or direct email over public feeds.
- Comments turned off on any public post carrying student images. Where a platform does not allow comments to be disabled, do not post student images to it.
- Tagging and location tagging disabled. No geotags on any post involving students.
- Public social channels reviewed annually against the platform's current terms: what licence does posting grant the platform, does it permit AI training use, and does it permit downstream licensing?
- No student images on unofficial, personal, booster-run, team-run, or classroom-run accounts that the school does not administer. Either bring the account under school administration or it does not carry student images.
- Search-engine indexing considered: image directories, staff pages, and athletics archives should be reviewed for whether they need to be indexable at all.

Record

- Log every public publication: image reference, purpose, channel, consent status of every identifiable person, publishing staff member, publish date, review date, planned takedown date.
- Keep the log in a searchable system, not in someone's inbox. When a family asks for removal, the log is what makes removal possible within hours instead of weeks.
- Record takedown requests, actions taken, dates, and outcomes, including where removal was not technically possible and why.

Ongoing review

- Annual review of all public image content on the school website, every social channel, digital and print yearbooks, athletics archives, grant and marketing collateral, and third-party platforms. Delete anything without ongoing purpose, consent, or accuracy.
- Annual re-consent cycle, communicated to families in the first two weeks of the school year alongside the annual FERPA notice.
- Annual platform-settings audit: privacy controls, commenting, tagging, sharing, download permissions, archive visibility, admin access list, and removal of former staff from admin roles.
- Annual staff refresh: a short training module and a signed acknowledgement, extended to coaches, volunteers, substitutes, aides, and contractors.
- Exposure audit of what is publicly discoverable about your school: search your own school name, mascot, and staff names in image search and see what comes back.
- Register of image incidents, near-misses, and takedown requests. Trend review each term; annual report to the governing board.

9 Athletics, livestreams, yearbooks, and third-party platforms

These four settings account for the majority of exposure in most U.S. schools, and they are usually governed by nobody. Treat each as a named owner's responsibility under this policy.

Athletics and activities

- Rosters are the problem, not just the photos. A public roster with full name, jersey number, grade, height, and position, published next to an action photo, gives an offender identity, age, school, and appearance in one place. Publish first name and last initial, or jersey number only, unless there is a specific consented reason.
- Booster clubs, team parents, and individual coaches must not run image-carrying accounts outside school administration.
- Away games and tournaments: your consent register does not bind the opposing school, the venue, the league, or attending families. Brief students that images may be captured by others, and give them a route to report it.
- Athletic trainer, injury, and medical images are health records, not communications assets. They never go on a public channel.
- Team photo days follow the professional-photographer rules in Section 7 without exception.

Livestreaming and video

- Livestreaming multiplies the risk: continuous frames, many angles, clear faces, timestamped, with a persistent archive. Apply a higher consent threshold than for stills, and obtain specific livestream consent.
- Fix the camera position to wide play rather than tracking individual children. No close-up crowd or bench panning.
- Turn off automatic archiving, or set a short retention period. An archived season is a face database.
- Disable chat and comments, or do not stream. Moderated chat on a stream featuring minors is a full-time job nobody is doing.
- Check the streaming vendor's terms for AI training, model improvement, facial recognition, highlight-generation, and downstream licensing rights. Many sports-streaming platforms use automated player recognition, that is biometric processing of children and needs explicit, informed consent and a legal review.
- Announcers must not read out full student names, grade levels, and hometowns on a public stream as a matter of routine.

Yearbooks and school publications

- Digital yearbooks are permanent, indexable, high-resolution, and name-labelled, the single richest source of student images most schools produce. Restrict access behind authentication; do not publish the yearbook as an open PDF.
- Names paired with faces are the core function of a yearbook, which is exactly why the channel must be closed rather than public.
- Apply the opt-out register to the yearbook, and make clear to families at consent time that yearbook is a separate tick box.
- Student journalism has genuine editorial independence considerations. Brief student editors on this policy rather than overriding them, and agree a protocol for image selection and takedown requests in advance.

Third-party platforms, apps, and AI tools

- Any platform that receives student images, classroom communication apps, portfolio apps, photo-sharing services, sports platforms, AI photo tools, print vendors, translation and design tools, requires a documented review before use.

- Ask, in writing: where are images stored, who can access them, are they used for AI training or model improvement, is facial recognition applied, what is the retention period, what happens on contract termination, and what is the deletion mechanism?
- Under COPPA as amended in 2025, where the school authorises collection from students under 13, consent must be specific to the platform and the purpose, retention must be limited, and a written data-retention policy is expected. School-provided consent does not cover uses beyond the educational purpose.
- Never upload a student image to a consumer AI tool, image generators, editors, upscalers, background removers, avatar makers, or chat assistants, without an executed agreement covering student data. "Just to tidy up the photo" is a data disclosure.
- Maintain a single approved-platform list. If it is not on the list, student images do not go into it.

10 Vendors and contracts

The clauses below are drafting starting points for district counsel, not executed language. Insert them in every contract, purchase order, memorandum of understanding, or volunteer agreement under which a third party may capture, receive, store, or process images of students or staff.

Clause	Required effect
Purpose limitation	Images may be used solely for the purpose specified in the written brief, and for no other purpose, including the vendor's own marketing, portfolio, competition entries, case studies, or stock libraries.
AI and model training prohibition	The vendor shall not use, disclose, or permit any third party to use the images to train, fine-tune, evaluate, or improve any machine-learning or artificial-intelligence model, and shall not submit the images to any generative-AI service. This survives termination.
Biometric prohibition	The vendor shall not apply facial recognition, facial-matching, age-estimation, emotion-detection, or other biometric processing to the images without the school's prior written authorisation and documented parental consent.
Handover and deletion	All original files shall be delivered to the school tenant by a stated date; the vendor shall then permanently delete all copies, including backups and cloud caches, and certify deletion in writing.
No sub-processing	No subcontracting, offshoring, or onward transfer without prior written approval and flow-down of these clauses.
Security and breach notification	Stated security controls, and notification to the school within a stated short period – 24 or 48 hours – of any actual or suspected unauthorised access, with cooperation in the school's own notification duties.
FERPA school-official status	Where applicable, the vendor is designated a school official under FERPA's exception, is under the school's direct control regarding use and maintenance of education records, and may not redisclose.

Clause	Required effect
State student-privacy compliance	Compliance with the applicable state student-data-privacy statute, expressly named, including any prohibition on targeted advertising, profiling, or sale of student data.
Takedown cooperation	The vendor shall action a school takedown or deletion request within a stated short period, including removal from published, cached, and archived locations under its control.
Indemnity and audit	Indemnity for breach of these clauses, and a right for the school to audit or require written attestation of compliance annually.

THE CLAUSE SCHOOLS MOST OFTEN FORGET

The AI-training prohibition. A school can do everything else correctly and still have a photographer, a streaming vendor, a yearbook platform, or a design tool lawfully feeding thousands of children's faces into a model under standard terms of service, because nobody said they could not.

11 When something goes wrong

DO THIS FIRST, IN THIS ORDER

- 1 Protect the child** Check on the student and family. If a criminal offence is possible, do not view, forward, download, print, screenshot the material itself, or store it. Do not ask the student to show you the image.
- 2 Notify** Escalate immediately to the principal or head of school, the designated safeguarding or student-services lead, the Title IX Coordinator where the incident may involve sex-based harassment, and the superintendent for anything district-level.
- 3 Report** Do not wait for an internal investigation. Make the mandated report to your state child-abuse hotline within the statutory timeframe, and call local law enforcement where there is an immediate safety concern. Reporting duties run in parallel with, not after, your internal process.
- 4 Preserve evidence lawfully** Record URLs, account handles, usernames, platform, times, and dates. Where CSAM or intimate-image abuse may be involved, do not save the material, record the location and let law enforcement direct evidence handling. Instruct staff and students not to delete devices or accounts before police advise.
- 5** File a CyberTipline report to the National Center for Missing and Exploited Children, and use Take It Down for nonconsensual intimate imagery of a minor.
- 6** Issue platform takedown notices under the TAKE IT DOWN Act removal process, covered platforms must remove a reported nonconsensual intimate visual depiction, and known identical copies, within 48 hours of a valid request.
- 7** Support the student and family. A single named staff contact, counselling or mental-health involvement, academic and attendance adjustments, supportive measures under Title IX, a safety plan, and a communications plan agreed with the family. Do not discipline, isolate, or relocate the targeted student to manage the problem.

- 8 Review** What changed the risk? Which image, channel, roster, platform, contract, or process must change permanently? Record it in the incident register and report the change to the board.

National reporting lines

- Your state child-abuse hotline, every state makes school personnel mandated reporters. Insert your state's number and statutory timeframe from Section 5. The Childhelp National Child Abuse Hotline, 1-800-422-4453 (call or text), can route a caller who does not know their state number, and the Child Welfare Information Gateway lists state reporting numbers.
- Local law enforcement for any immediate safety concern, and your regional ICAC Task Force, a national network of 61 task forces, for suspected AI-generated CSAM, sextortion, or coerced intimate imagery of students.
- FBI, including tips.fbi.gov and the local field office, for sextortion, interstate offenders, and financially motivated sextortion schemes.
- NCMEC CyberTipline at report.cybertip.org, available to all staff and frequently required in parallel with child-welfare and law-enforcement reporting. AI-generated child sexual abuse material is treated as child sexual abuse material; federal law reaches computer-generated and manipulated depictions.
- NCMEC Take It Down at takeitdown.ncmec.org for removal of nonconsensual intimate images of people who were minors at the time. For adults, including staff, StopNCII.org performs the equivalent function.
- Platform reporting under the TAKE IT DOWN Act, covered platforms must provide a removal-request process and remove within 48 hours of a valid request. The FTC enforces this obligation and accepts complaints at ReportFraud.ftc.gov.
- Your county prosecutor or district attorney and state attorney general, where your state NCII, deepfake, CSAM, or juvenile-sexting statutes may apply.
- Your Title IX Coordinator, where the incident involves sex-based harassment between students, or by or against staff. Every recipient of federal funds must designate one.
- U.S. Department of Education Student Privacy Policy Office for suspected FERPA violations, and your state education agency privacy office where the state has one.
- 988 Suicide and Crisis Lifeline, call, text, or chat, plus your school counsellors, school psychologists, and your state youth crisis line. Image-based abuse carries a significant self-harm risk; treat wellbeing as a parallel workstream from hour one.

Common pitfalls to avoid

- Staff or leaders viewing, forwarding, downloading, or "keeping a copy" of suspected illegal material to assess how bad it is. This can itself be a criminal offence, however well intentioned.
- Deleting or instructing a student to delete material before law enforcement have advised on preservation.
- Contacting the suspected perpetrator, their family, or the account directly instead of going through law enforcement.
- Treating an AI-generated image as "not real" and therefore not a safeguarding matter. It is a safeguarding, Title IX, and mandated-reporter matter regardless of how it was produced.
- Running the incident purely as a discipline matter, which misses the mandated report, the Title IX obligation, and the criminal referral.

- Punishing, excluding, or transferring the targeted student to reduce disruption. This is the single most damaging pattern in documented U.S. school cases.
- Missing the statutory reporting window while an internal investigation proceeds. Report first; investigate in parallel.
- Failing to notify affected students and families on the assumption that less said is better. Assume they will find out, and that how you told them will be the story.
- No plan for the wider cohort: other students have usually seen the material and need support and clear messaging too.
- Waiting for perfect information before issuing takedown notices. Notices can be issued while facts are still being established.

12 Federal legal and regulatory map

Instrument	What it requires of U.S. schools
FERPA – 20 U.S.C. 1232g; 34 CFR Part 99	A photograph or video of a student is an education record when it is directly related to a student and maintained by the school. It may be disclosed without consent only if photographs have been designated as directory information in the annual notice and families were given a meaningful opportunity to opt out. Coupling an image with protected information – grades, discipline, IEP or 504 status, English-learner or McKinney-Vento status – always requires written consent. Rights transfer to eligible students.
COPPA – 15 U.S.C. 6501–6506; 16 CFR Part 312, as amended 2025	Where the school authorises a third-party operator to collect images or identifiers from students under 13, consent must be verifiable and specific to that platform and purpose. The 2025 amendments, effective June 2025 with full compliance required by April 2026, expand the definition of personal information, tighten retention, and require a written data-retention policy.
Title IX – 20 U.S.C. 1681; 34 CFR Part 106	Sex-based harassment carried out through image manipulation – between students, or by or against staff – triggers Title IX response obligations, supportive measures, and grievance procedures. As at September 2026 the 2020 regulations are operative nationwide following the January 2025 vacatur of the 2024 rule. Every recipient must designate a Title IX Coordinator.
TAKE IT DOWN Act – 2025	Creates a federal criminal offence for knowingly publishing nonconsensual intimate visual depictions, expressly including AI-generated or digitally forged depictions, with enhanced treatment where the person is a minor. Requires covered platforms to provide a removal-request process and to remove a reported depiction and known identical copies within 48 hours of a valid request. FTC enforcement of the platform duty began 19 May 2026.

Instrument	What it requires of U.S. schools
DEFIANCE Act of 2024	Creates a federal civil cause of action for victims of nonconsensual digital forgeries, allowing victims to sue those who produce, disclose, or solicit such material. Relevant to how you advise families on their options, and to your own litigation exposure.
18 U.S.C. 2251, 2252A – child pornography offences	Production, distribution, receipt, and possession offences. Federal CSAM law reaches computer-generated and manipulated depictions, including where the depicted minor is identifiable from an ordinary school photo.
18 U.S.C. 1466A – obscene visual representations of the sexual abuse of children	Reaches drawings, cartoons, sculptures, paintings, and computer-generated images depicting minors in sexually explicit conduct that are obscene or lack serious value, without requiring an actual child to have been depicted.
18 U.S.C. 2258A – provider reporting duty	Electronic service providers must report apparent child sexual exploitation to the NCMEC CyberTipline. This is why platform and school reports converge at NCMEC, and why your report there is useful even when the platform has also reported.
Section 504 and the ADA	Publishing an image that reveals disability status, placement, or service receipt without consent is both a FERPA and a disability-privacy problem. Targeting of a student with a disability may also trigger disability-harassment obligations.
PPRA – 20 U.S.C. 1232h	Governs surveys and certain information collection from students; relevant where image collection is bundled with survey, research, or marketing activity.
State law – see Section 13	Mandated reporting, NCII, synthetic intimate imagery, AI-generated CSAM, juvenile sexting, student records confidentiality, student-data-privacy vendor duties, and biometric privacy. Localise using the worksheet in Section 5.

FEDERAL LAW IS THE FLOOR, NOT THE CEILING

Almost every consequence a school actually faces after an image incident is generated by state law and local process: the mandated-report failure, the prosecutor referral, the state privacy-office determination, the state civil claim, the board complaint, and the licensure question for the staff member who handled it badly. District counsel must map your state's specific statutes and timeframes onto the workflow in Section 11 before this document is adopted.

13 The state-law layer

The point of this section is not to reproduce fifty statutes, which change every legislative session. It is to tell you exactly which categories to check, what good looks like in each, and where to verify the current position.

Category	What to check in your state	Position nationally, as at September 2026
Mandated reporting	Which school staff are covered, what triggers the duty, the statutory timeframe, the correct hotline, and whether reporting to a supervisor satisfies the duty (usually it does not).	All states make school personnel mandated reporters, but wording, timeframes, and hotlines differ. Many states require a report immediately or within 24 hours.
AI-generated or computer-edited CSAM	Whether your state statute expressly covers AI-generated, morphed, or computer-edited depictions, and whether it requires an identifiable real child.	ENOUGH ABUSE records 46 to 47 states with such statutes as at 2026, with a small number of states and D.C. still without one. Most were enacted from 2024 onwards.
Nonconsensual intimate imagery	Whether your state NCII statute covers digitally created or altered images, and whether minors are addressed separately.	Independent trackers record 48 states addressing sexually explicit deepfakes in some form, with more than 250 deepfake-related statutes nationwide.
Juvenile sexting and peer-to-peer conduct	Whether there is a graduated or diversion pathway for students, and what the prosecutor's practice actually is.	Many states have juvenile-specific provisions to avoid charging children with felony CSAM offences. Practice varies sharply by county.
Student records confidentiality	Your state FERPA analogue in the education code, and any stricter consent requirement for photographs.	Most states have one; several are stricter than FERPA on images and on disclosure logging.
Student data privacy and vendor duties	Your SOPIPA-style statute: prohibitions on targeted advertising, profiling, sale of student data, and required deletion on request.	At least 40 states have enacted student-privacy statutes since 2013. These bind vendors directly, so a FERPA-compliant vendor can still be non-compliant in your state.
Biometric privacy	Whether facial recognition or facial matching by a vendor is restricted or prohibited, and whether school use of facial recognition is regulated.	Several states restrict biometric identifiers, and a number restrict or prohibit facial recognition in schools specifically. Check before approving any player-recognition or auto-tagging feature.
Comprehensive consumer privacy law	Whether your state's consumer privacy act carries obligations relevant to your vendors, even where education data is exempt.	A growing majority of states now have comprehensive privacy statutes with varying education exemptions.
Age-appropriate design and minors' online safety	State duties on platforms that may create reporting or escalation routes for your families.	A fast-moving area with active litigation; useful to know what leverage families have.

HOW TO KEEP THIS CURRENT

Assign a named owner, usually general counsel or the privacy officer, to re-verify Section 5 and Section 13 every twelve months and after each legislative session. Record the verification date on the cover of your adopted version. A document that claims to state the law and has not been checked in two years is worse than no document.

14 Roles and accountability

A rule without a named owner is a rule that lapses. Assign every row below to a named individual, record the name in your adopted version, and review at least annually. Small schools may combine roles, but every row must have a name against it.

Role	Ownership
Superintendent / Head of School	Owns this policy; signs off on the annual review; final decision-maker on school-wide incidents; reports to the governing board.
Governing Board / Board of Trustees	Approves the policy; receives the annual report on image incidents, takedowns, consent completion, and privacy compliance; holds leadership accountable for the six metrics in Section 15.
General Counsel / District Counsel	Owns the localisation worksheet in Section 5, verifies Section 13 annually, approves the vendor clauses in Section 10, and advises on evidence handling and law-enforcement liaison.
Privacy Officer / FERPA Officer	Owns directory-information designation, the annual FERPA notice, the opt-out register and its accessibility to staff at point of capture, consent records, and privacy-incident response.
Title IX Coordinator	Primary owner where an incident may involve sex-based harassment through image manipulation; supportive measures, grievance procedure, and timelines.
Designated safeguarding / student-services lead	Owns the higher-care list in Section 7, the mandated-report decision and record, and the student and family support plan.
Communications / Marketing lead	Owns the publishing workflow, channel selection, metadata stripping and downscaling, comments-off enforcement, the publication log, the annual public-content audit, takedown execution, and platform notices.
Chief Technology Officer / IT Director	Owns device management and enrolment, tenant storage security and retention, access control, the approved-platform list, vendor security review, network-level filtering of nudity and deepfake generation services, and evidence preservation support.
Athletic Director	Owns rosters, team and booster accounts, livestream configuration and retention, streaming-vendor terms, away-game briefing, and coach training under this policy.

Role	Ownership
Principal / Building administrator	Owens local implementation, staff and volunteer training completion, the in-the-moment culture, and first-response coordination during an incident. Mandated reporter.
Classroom teachers, coaches, paraprofessionals, volunteers, substitutes	Own in-the-moment consent, safe framing, correct device use, and escalation. All are mandated reporters where state law so provides.
Yearbook and student publications advisor	Owens yearbook access control, opt-out application, and the protocol agreed with student editors.
School counsellors, social workers, psychologists, nurses	Support the affected student and family; coordinate the mental-health response with 988 and community providers; monitor the wider cohort.
School Resource Officer, where present	Liaison with local law enforcement and the regional ICAC Task Force. Not a substitute for the mandated report to the state hotline.
Students	Entitled to decline on the day, to be told how their images are used, and to report concerns without fear of discipline. Named here because a policy children do not know about does not protect them.

15 Board-level assurance

Twelve-month calendar

When	What happens	Owner
Before the school year starts	Localisation worksheet re-verified; policy version dated; staff and volunteer training module released; approved-platform list refreshed.	Counsel, Privacy Officer, IT
First two weeks of term	Annual FERPA notice issued with photographs designated or not; channel-specific consent issued to every family; opt-out register rebuilt and published to staff.	Privacy Officer
End of first term	Consent completion rate reported; gaps chased; incident register reviewed for trends.	Privacy Officer, Communications
Mid-year	Public-content audit of website, all social channels, athletics archives, and yearbook access; platform-settings and admin-access audit; former-staff admin removal.	Communications, IT
Mid-year	Livestream and athletics review: retention settings, roster detail, vendor terms, booster accounts.	Athletic Director
Each term	Incident, near-miss, and takedown register reviewed; lessons recorded; process changes made.	Safeguarding lead

When	What happens	Owner
Annually	Tabletop exercise: a fabricated explicit image of a named Year 9 student is circulating at 7:40 am on a Monday. Run the full Section 11 workflow against the clock.	Head of School
Annually	Board report against the six metrics below; policy approved or amended; named owners confirmed.	Head of School, Board

The six metrics to report to your board

- **Consent completion rate** – Percentage of enrolled students with a current, channel-specific consent record, and percentage of staff with a signed acknowledgement of this policy.
- **Public image inventory** – Number of identifiable student images currently published on each public channel, and the change since last year. A reduction is a good outcome, not a communications failure.
- **Log coverage** – Percentage of public images with a complete log entry, named owner, and review date.
- **Incidents and near-misses** – Number, type, source channel, time to report to the state hotline, time to takedown request, time to actual removal.
- **Takedown performance** – Requests made, removals achieved, removals not achieved and why, and average time to removal.
- **Training and audit currency** – Percentage of staff, coaches, and volunteers trained in the last twelve months; date the localisation worksheet was last verified; date of the last public-content audit.

WHAT "GOOD" LOOKS LIKE AFTER A YEAR

Fewer published images, all of them logged and consented. A visible drop in identifiable close-ups and name-plus-face pairings. An opt-out register the person holding the camera can check in ten seconds. A tabletop exercise completed, and the gaps it found closed. A board that has seen the numbers and asked about them.

16 One-page checklist

Print, laminate, and distribute to every classroom, athletics office, front desk, main office, library, and to every coach, volunteer, and substitute.

Before you take an image

- Purpose is clear and cannot be met by a lower-risk alternative.
- Consent is current, informed, and channel-specific, cross-checked against the opt-out register.
- No student in frame is on the higher-care list or has indicated they do not want to be photographed today.
- School-owned device, images landing in the school tenant.
- Framing minimises identifiability, wide, activity-focused, side-on.

Before you publish an image

- Wider shot, activity over face, no unsafe or compliance-sensitive detail visible.
- No student name paired with a face; no uniform plus location plus name combination; no roster detail alongside.

- Metadata stripped, resolution reduced, filename anonymised, alt text describes the activity.
- Least-public channel that serves the purpose; comments and tagging off.
- Log entry created with named owner, review date, and takedown date.

If misuse is suspected

- Do not view, download, screenshot, or forward suspected illegal material.
- Escalate immediately to the principal, the designated safeguarding lead, and the Title IX Coordinator where relevant.
- Make the mandated report to your state child-abuse hotline within the statutory timeframe, insert your number here: _____. Call local law enforcement for any immediate safety concern, and your regional ICAC Task Force for suspected AI-generated CSAM or sextortion.
- File an NCMEC CyberTipline report at report.cybertip.org; use takeitdown.ncmec.org for a minor, StopNCII.org for an adult.
- Issue platform takedown notices under the TAKE IT DOWN Act removal process, 48 hours from a valid request.
- Support the child and family. Do not discipline or isolate the targeted student. Document everything.

17 Family-facing summary

Paste this into your newsletter, family handbook, or enrolment pack. Replace the bracketed text.

FOR FAMILIES

We celebrate your child's achievements in ways that also protect their long-term privacy. Photos and video are only ever taken for a clear educational or communications reason, on school-owned devices, by staff who have read and signed our image policy.

We prefer wider shots over close-ups, and we do not publish your child's name alongside their photo unless you have specifically agreed to it. Before anything goes onto a public channel, we remove the hidden location and device information from the file, reduce the image size, and choose the most private channel that still does the job.

You control what you consent to, and you can change your mind at any time. Every year, alongside our annual Family Educational Rights and Privacy Act notice, we ask you to review your image preferences. Internal school use, our website, social media, news media, yearbook, and livestreamed events each have their own tick box.

If your child says "not today" on the day of an activity, we respect that without question or consequence, even if you have signed the annual consent form. Your child will never be moved aside, named to the group, or left out of the activity.

AI tools have made it easy to alter or fabricate images of children, including from an ordinary school photo. That is why we publish fewer images, review every public channel each year, and delete images that no longer serve a purpose. It is also why we ask our photographers, yearbook providers, and streaming services in writing never to use images of your child to train AI systems.

If you are ever worried about an image of your child online, tell us. You will not be judged, and your child will not be in trouble. We will act the same day: we will investigate, request removal, support your family through any report to [state child protection hotline], [local police department], and the National Center for Missing and Exploited Children, and we will tell you honestly what we can and cannot get taken down.

If your child has already been affected, you can request removal yourself at takeitdown.ncmec.org. Adults, including staff, can use StopNCII.org. You can also contact us for help doing it, and you can reach the 988 Suicide and Crisis Lifeline at any hour by call, text, or chat.

18 Model consent form

Reproduce on school letterhead. Issue annually, in the first two weeks of the school year, alongside the annual FERPA notice, and in the languages your community uses.

Student and family details

Student name	Grade / homeroom	School year
--------------	------------------	-------------

Parent or guardian name	Relationship
-------------------------	--------------

Where the student is 18 or older, or attends a postsecondary institution, rights under FERPA have transferred and the student signs this form themselves.

Please tick the channels you agree to. You may tick some, all, or none.

Channel	What it means	Yes	No
Internal school use only	Classroom displays, internal newsletters sent only to our families, and the parent portal or learning management system.	☐	☐
School website	Our public website, visible to anyone on the internet and indexable by search engines.	☐	☐
School social media	Our official, school-administered accounts. Comments are turned off on posts featuring students.	☐	☐
News media	Photographs or footage supplied to newspapers, television, or online news outlets. We cannot control reuse once supplied.	☐	☐
Yearbook and school publications	Our yearbook and student publications, where names normally appear alongside photographs.	☐	☐
Livestreamed events	Live video of assemblies, performances, or athletics events. Archives are kept for no more than [period].	☐	☐
Enrolment and marketing materials	Prospectus, brochures, advertising, open-day displays, and grant or funding reports.	☐	☐
Name alongside image	Whether your child's first name may appear with their photograph on any channel you have agreed to above. We never publish full names with photographs.	☐	☐

Restrictions and requests

Are there any restrictions, sensitivities, or circumstances we should know about? You do not need to give a reason for any request to limit or withhold consent.

What you are agreeing to, and what you are not

- This consent covers the current school year only and is refreshed every year.
- You can withdraw or change your consent at any time, in writing or by contacting [named contact]. We will stop using the image on any channel we control, and remove it where removal is technically possible. We will tell you honestly where it is not.
- If your child declines to be photographed on the day of an activity, we will respect that, whatever this form says.
- We never publish your child's photograph alongside protected information such as grades, class placement, disability or special education status, disciplinary matters, English-learner status, or housing status.

- We require our photographers, yearbook providers, and streaming services in writing not to use images of your child for AI training, facial recognition, portfolios, marketing, or stock libraries.
- We cannot control images captured by other families, spectators, opposing schools, or the public at events open to the community. We ask everyone to be considerate and we brief students accordingly.

Signature _____

Print name _____

Date _____

Questions, withdrawals, and takedown requests: [named role], [email], [phone].

19 Sources and further reading

Federal law and guidance

- **U.S. Department of Education** – FERPA, Protecting Student Privacy: <https://studentprivacy.ed.gov/ferpa>
- **U.S. Department of Education** – FAQs on Photos and Videos under FERPA: <https://studentprivacy.ed.gov/faq/faqs-photos-and-videos-under-ferpa>
- **U.S. Department of Education** – Title IX and sex discrimination, overview of the law: <https://www.ed.gov/laws-and-policy/civil-rights-laws/title-ix-and-sex-discrimination/sex-discrimination-overview-of-law>
- **Congressional Research Service** – Status of the Education Department's Title IX regulations: <https://www.congress.gov/crs-product/LSB11279>
- **FTC** – Complying with the TAKE IT DOWN Act: <https://www.ftc.gov/business-guidance/resources/complying-take-it-down-act>
- **FTC** – TAKE IT DOWN Act enforcement guidance for businesses: <https://www.ftc.gov/business-guidance/blog/2026/05/take-it-down-act-enforcement-starts-now-what-know-about-ftc-tida>
- **FTC** – TAKE IT DOWN Act statute page: <https://www.ftc.gov/legal-library/browse/statutes/tools-address-known-exploitation-immobilizing-technological-deepfakes-websites-networks-act-take-it>
- **FTC** – Children's privacy and COPPA business guidance: <https://www.ftc.gov/business-guidance/privacy-security/childrens-privacy>
- **18 U.S.C. 1466A** – obscene visual representations of the sexual abuse of children: <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section1466A&num=0&edition=prelim>
- **18 U.S.C. 2258A** – provider reporting requirements: <https://www.law.cornell.edu/uscode/text/18/2258A>
- **DEFIANCE Act of 2024** – S.3696: <https://www.congress.gov/bill/118th-congress/senate-bill/3696>
- **U.S. Department of Justice** – Citizen's guide to federal law on obscenity: <https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-obscenity>

Reporting, removal, and support

- **NCMEC CyberTipline** – <https://report.cybertip.org>
- **NCMEC Take It Down** – removal for people who were minors at the time: <https://takeitdown.ncmec.org>
- **StopNCII.org** – removal for adults: <https://stopncii.org>
- **Childhelp National Child Abuse Hotline** – 1-800-422-4453: <https://childhelpline.org/>

- **Child Welfare Information Gateway** – how to report child abuse and neglect, by state: <https://www.childwelfare.gov/how-report-child-abuse-and-neglect/>
- **Internet Crimes Against Children Task Force Program** – 61 task forces: <https://www.icactaskforce.org/>
- **OJJDP** – ICAC Task Force Program: <https://ojjdp.ojp.gov/programs/internet-crimes-against-children-task-force-program>
- **FBI** – submit a tip: <https://tips.fbi.gov>
- **988 Suicide and Crisis Lifeline** – <https://988lifeline.org>

Scale and evidence

- **NCMEC** – CyberTipline data: <https://www.missingkids.org/cybertiplinedata>
- **NBC News** – reporting on generative-AI CyberTipline volumes in 2025: <https://www.nbcnews.com/tech/security/ai-child-exploitation-crisis-rcna259409>
- **Internet Watch Foundation** – AI-generated child sexual abuse material, annual data insights 2025: <https://www.iwf.org.uk/annual-data-insights-report-2025/emerging-and-persistent-harms/ai-generated-child-sexual-abuse-material>
- **Fortune** – IWF finding of a 260-fold increase in AI-generated CSAM videos in 2025: <https://fortune.com/2026/04/03/internet-watch-foundation-260-fold-increase-ai-generated-csam/>
- **USA Today** – Lancaster, Pennsylvania school deepfake case, sentencing March 2026: <https://www.usatoday.com/story/life/health-wellness/2026/03/25/lancaster-country-day-school-students-sentenced-deepfake-porn/89299664007/>
- **Washington Times** – Louisiana middle-school case in which the targeted student was expelled: <https://www.washingtontimes.com/news/2025/dec/22/artificial-intelligence-deepfakes-nude-teenagers-upend-middle/>

State-law trackers to use with Section 5

- **ENOUGH ABUSE** – state laws criminalising AI-generated or computer-edited CSAM: <https://enoughabuse.org/get-vocal/laws-by-state/state-laws-criminalizing-ai-generated-or-computer-edited-child-sexual-abuse-material-csam/>
- **Student Privacy Matters** – state student privacy laws: <https://studentprivacymatters.org/state-legislation/>
- **Student Privacy Matters** – privacy bills by state chart: <https://studentprivacymatters.org/1908-2/>
- **Deepfake legislation tracker** – federal and state laws: <https://stackcyber.com/posts/ai-deepfake-laws>

Example of a state privacy determination on school social media photographs

- **New York State Education Department** – Brewster Central School District determination, April 2026: <https://www.nysed.gov/sites/default/files/programs/data-privacy-security/brewster-decision-4-3-26.pdf>
- **New York State Education Department** – Croton Harmon Union Free School District determination, September 2024: <https://www.nysed.gov/sites/default/files/programs/data-privacy-security/croton-harmon-determination-9.12.2024.pdf>