



School Response Checklist: Image-Based Abuse & Sextortion

For school and youth-serving professionals. This is a practice checklist, not legal advice. Real, edited and AI-generated intimate images can cause serious harm and should be handled with the same focus on safety, dignity, privacy and coordinated response.

Immediate response

- ☐ Move the student to a private, safe setting.
- ☐ Listen without blaming, shaming or asking the student to prove what happened.
- ☐ Assess immediate safety, threats, coercion, self-harm or suicide risk.
- ☐ Do not ask staff or students to forward the image to you.
- ☐ Preserve useful information such as usernames, links, dates and threats without unnecessary copying.
- ☐ Follow school policy and notify the designated administrator / safeguarding lead.

Coordinate

- ☐ Identify which caregiver / guardian should be contacted and any safety reason that affects contact.
- ☐ Consider Cybertip.ca / police reporting where appropriate.
- ☐ Use NeedHelpNow.ca for youth image-removal support.
- ☐ Create a school safety plan if peers are involved.
- ☐ Protect the student from repeated questioning and unnecessary disclosure.
- ☐ Arrange a check-in after the immediate incident.



School Response: Follow-up & Recovery

School environment

- ☐ Address rumours, harassment and peer retaliation without identifying the victim unnecessarily.
- ☐ Consider schedule, transportation, class, lunch or extracurricular safety needs.
- ☐ Identify one trusted school adult for ongoing check-ins.
- ☐ Document actions and responsibilities clearly.
- ☐ Do not treat an AI-generated sexual deepfake as harmless because the image is fake.
- ☐ Separate discipline of those causing harm from support for the impacted student.

Record

Student support lead

Caregiver contact

External report / reference

Safety-plan actions

Review date