



Association of
Title IX Administrators

Title IX in the Digital Age: Implications for K-12 Schools

2026 Keystone Title IX & Education Law Summit

WELCOME!

Step 1. Register here



Step 2. ATIXA Event Lobby (access to slides)





Any advice or opinion provided during this training, either privately or to the entire group, is **never** to be construed as legal advice or an assurance of compliance. Always consult with your legal counsel to ensure you are receiving advice that considers existing case law in your jurisdiction, any applicable state or local laws, and evolving federal guidance.

Daniel Swinton, J.D., Ed.D.

- Chief Consulting Officer and Partner, TNG/ATIXA
- Senior Resolution Officer, FAIR Center
- Daniel.Swinton@tngconsulting.com
- www.tngconsulting.com
- www.atixa.org



Content Advisory

The content and discussion in this presentation will necessarily engage with identity-based harassment, discrimination, violence, and associated sensitive topics that can evoke strong emotional responses.

ATIXA faculty members may offer examples that emulate the language and vocabulary that Title IX practitioners may encounter in their roles including slang, profanity, and other graphic or offensive language. It is not used gratuitously, and no offense is intended.

AGENDA

1

Definitions

2

Legal & Policy Framework

3

Best Practices for Response

4

Prevention and Education

Definitions

Technology-facilitated Sexual Abuse (TFSA)

- Gender-based abuse facilitated via the use of communication technology or emerging technology
 - Image-based abuse
 - Recorded Sexual Assault
 - Non-consensual intimate image sharing
 - Sexual extortion
 - Doxing
 - Cyberstalking
 - Cyberharassment
 - Intimate Partner Violence

Image-based Sexual Abuse

- The sharing or the threatening to share sexually explicit or intimate images of individuals without their consent.
 - Images originally obtained without consent
 - using hidden cameras
 - hacking phones
 - recording sexual assaults
 - Images consensually obtained within the context of a private intimate relationship that are later shared beyond the relationship
 - Non-consensual pornography
 - “Revenge porn”



Non-consensual Intimate Imagery (NCII)

- **Authentic NCII:**

- Authentic (i.e., real) sexually explicit, nude, or intimate videos, photos, or audio recordings of an individual,
- distributed without the consent of the individual depicted

- **Synthetic NCII:**

- Videos, photos, or audio representations of an individual that have been digitally manipulated (i.e., faked)
- to depict an individual in a sexually explicit, nude, or intimate manner or saying sexual or explicit words/statements,
- distributed without the consent of the individual depicted

Synthetic NCII depicts sexually related actions or behaviors that never happened, or places identifiable individuals in pornographic, nude, or sexual situations without their consent

Sexual Extortion

- Threatening to expose harmful sex-based information unless an individual engages in unwanted sexual conduct.
 - Provide nude or sexually explicit images
 - Perform sex acts
 - Pay an amount of money (ransom)
- Conditioning an aid, benefit, or service on an individual's engagement in unwanted sexual conduct
 - Abuses of power or authority
- A form of sexual exploitation that uses coercion tactics to gain or continue sexual access

Doxing

- The act of publishing identifiable private or personal information on the internet without the individual's consent.
 - Information originally obtained without consent (e.g., hacking, phishing scams)
 - Information consensually obtained within the context of a private relationship that is later used to inflict harm
- Often overlaps with other forms of technology-facilitated sexual abuse (i.e., image-based abuse, sextortion, cyberstalking, cyberharassment, IPV)

Cyberstalking

- Use of communication **technology**, or any other emerging technologies, to engage in a **course of conduct** directed at a specific person that would cause a reasonable person to –
 - Fear for that person’s safety or the safety of others, or
 - Suffer substantial emotional distress
- Most cyberstalking behaviors are **not** protected by the First Amendment
- If cyberstalking is sex- or gender-based, it may implicate **Title IX**



Forms of Cyberstalking

Passive

- Obtaining publicly available information without detection

Invasive

- Deliberate acts intended to infringe upon or violate privacy

Duplicitious

- Deceptive acts used to gain access to information without detection

Common Cyberstalking Tools and Tactics

- Artificial Intelligence (AI)-generated images and messaging
- Email
- Geo-positioning data or GPS via phones or cars
- Messaging apps
- Ransomware, viruses, spyware, and keystroke loggers
- Releasing personal data (Doxing)
- Sextortion
- Smart Home devices
- Surveillance via mobile devices
- Social media sites
- Social networking platforms
- Text messages

Cyberharassment

- The use of communication technologies, or any other emerging technologies to harass or bully another person
 - Most often occurs on social media platforms or other online forums
 - Also called cyberbullying



Bullying & Cyberbullying

- **Bullying** is unwanted, aggressive behavior that involves a real or perceived power imbalance. The behavior is often repeated or has the potential to be repeated over a period of time.
 - Verbal bullying
 - Social bullying
 - Physical bullying
- **Cyberbullying** is bullying that takes place over digital devices.
 - Includes sending, posting, or sharing negative, harmful, mean or false content about someone else.
 - Can overlap with forms of TFSA (e.g., NCII, doxing)

Source: www.stopbullying.gov

Key Differences

Cyberstalking

- Cause fear
- Maintain power and control
- Single perpetrator
- Perpetrator is often known to the Complainant
- Continuous cycle of incidents with multiple tactics

Cyberharassment

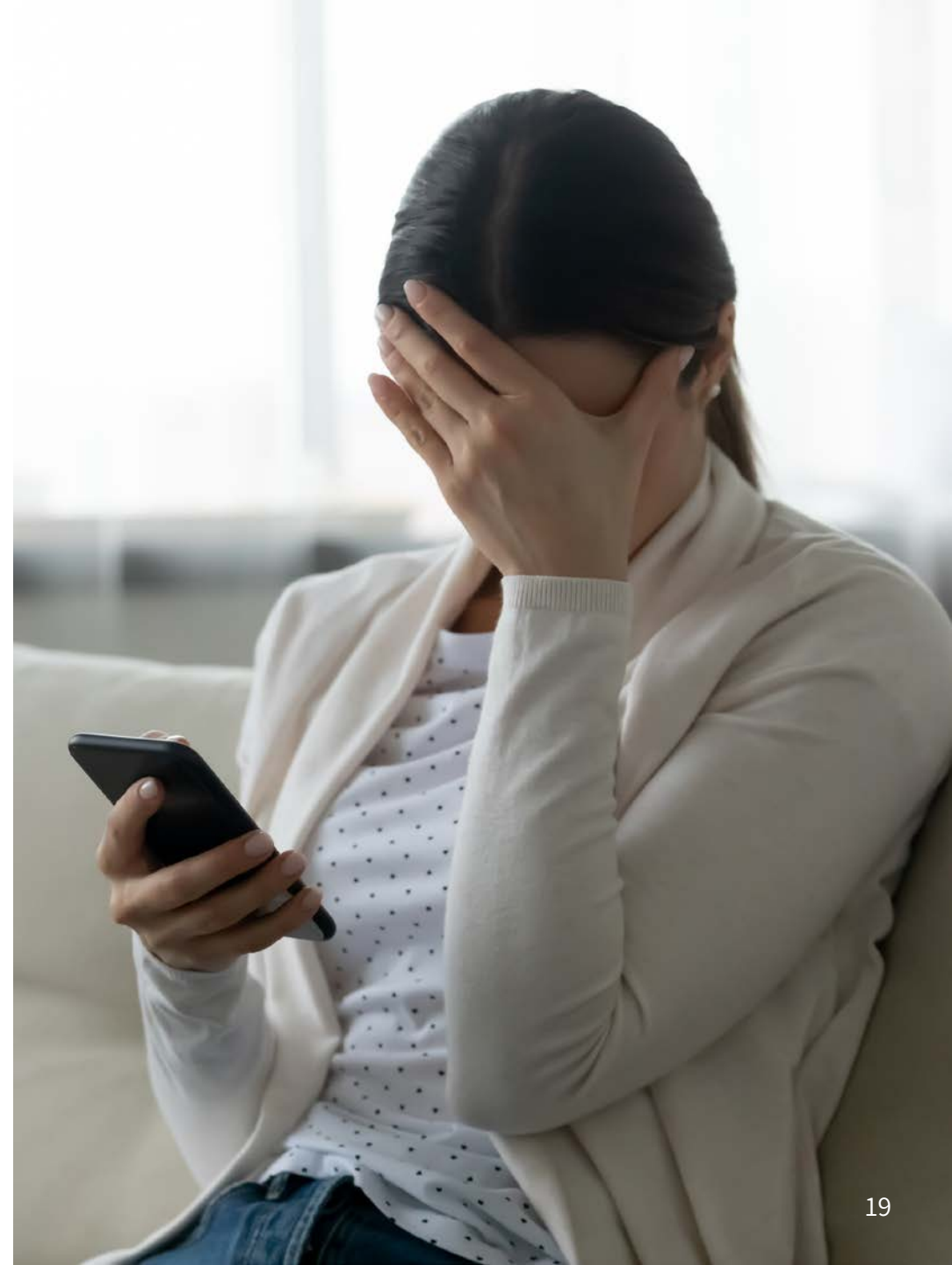
- Inflict harm
- Denigrate and/or humiliate
- Single or multiple perpetrators
- Perpetrators can be known, a stranger, or anonymous
- Often contained to a point in time with consistent tactics

Cyberbullying

- To harm or be mean
- Embarrass and/ or humiliate
- Often a single perpetrator
- Perpetrator is known
- Behavior is repeated over a period of time

Unique Challenges

- **Typically involves:**
 - Perpetrator anonymity/impersonation
 - Conduct outside-of-school control/jurisdiction, including mixed jurisdictional situations
 - Rapid spread and amplification
- Access to appropriate supportive measures and resources
- NCII of individuals under the age of 18 qualifies as Child Sexual Abuse Material (CSAM)



ATIXA's Recommended Best Practices

- Offer specialized training on NCII for Title IX team members, teachers, staff, and administrators
- Develop age-appropriate training and prevention education for students and parents/guardians
- Incorporate trauma-informed practices into response efforts
- Work closely with school resources officers (SROs) to appropriately manage NCII depicting minors
 - May qualify as CSAM
 - May trigger additional state law mandatory reporter obligations

Legal & Policy Framework

Title IX

“No person in the United States shall, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education program or activity receiving federal financial assistance.”

20 U.S.C. § 1681 & 34 C.F.R. Part 106 (1972)

Title IX has always mandated a response to sex discrimination, however the 2020 Title IX Regulations **only** apply to sexual harassment complaints



Essential Compliance Elements

The requirements to **Stop, Prevent,** and **Remedy** guide Title IX Coordinators (TIXCs) in their compliance work

1

STOP discriminatory conduct

2

PREVENT recurrence, on both individual and institutional levels

3

REMEDY the effects of discrimination, on both individual and institutional levels

Scope

Title IX

Sex Discrimination

- Disparate Treatment
- Program Equity

Retaliation

Sexual Harassment

- Quid Pro Quo
- Hostile Environment
- Sexual Assault
- Dating Violence
- Domestic Violence
- Stalking

Hostile Environment Sexual Harassment

- Unwelcome conduct
- determined by a reasonable person
- to be so **severe, pervasive, and objectively offensive (SPOO)**
- that it effectively denies a person equal access to the Recipient's education program or activity



Stalking

- Engaging in a course of conduct,
- On the basis of sex,
- Directed at the Complainant, that
 - would cause a reasonable person to fear for that person's safety, or
 - The safety of others, or
 - suffer substantial emotional distress

Retaliation: ATIXA Model Definition

- Recipient, or any member of Recipient's community,
 - Taking or attempting take materially adverse action,
 - By intimidating, threatening, coercing, harassing, or discriminating against any individual,
- For the purpose of interfering with any right or privilege secured by law or Policy, or
- Because the individual has made a report or complaint, testified, assisted, or participated or refused to participate in any manner in an investigation, proceeding, or hearing under this Policy and procedure

Best Practices for Response

Complaint Intake

- Gather information from Complainant and/or parent/guardian
 - Often reported by a third party
 - If connected to IPV, Complainants may minimize/excuse incidents and their impact
- Offer available supportive measures, including community-based options
- Ascertain safe communication methods that an abuser or stalker will not be able to access
- Assist the Complainant in reporting the conduct to appropriate school officials or local law enforcement
 - Consider any additional reporting responsibilities to law enforcement/protective services (if applicable)
- Provide opportunity to make a complaint
- Consider BIT/BTAM referral

Examples of Supportive Measures

- Classroom, housing (if applicable), or work arrangement adjustments
- Emergency notification
- Safety escorts
- Safety planning
- No Contact Orders
- Cease & Desist Directives
- Increased security and monitoring
- Referral to school counselors or Employee Assistance Program
- Trespass or “be on the lookout” (BOLO) orders
- Emergency funding

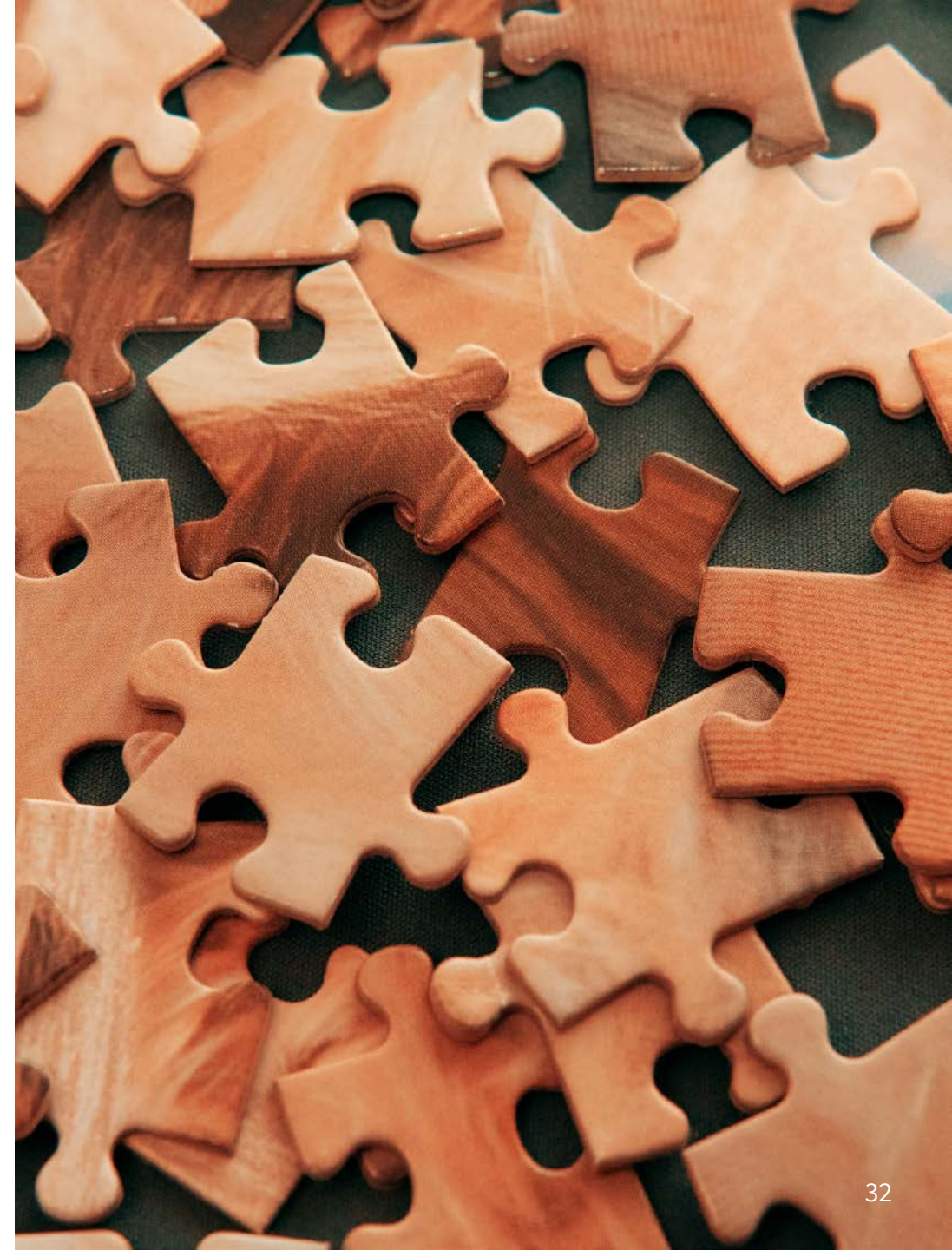
Safety Plans (Stalking)

- **Safety Plan:** a personalized, practical set of actions that can help lower risk for harm while experiencing abuse, preparing to leave an abusive situation, or after you leave
 - Includes information specific to the Complainant and their life that will increase their safety at school, home, and other places they visit routinely
 - Outlines necessary actions and available resources
 - Accounts for children and pets as applicable
- Complainant should keep a printed copy in a safe place, if possible, and provide a copy to a trusted friend or family member
- May require revision as circumstances change

Safety Planning Considerations

TIXC should engage in safety planning that considers:

- Level of access to the Complainant
- Full history of the alleged behaviors and context of the relationship
- Available support person(s) and immediate school-based resources
- Community-based resources
- Law enforcement or civil support options
- Readiness to leave and not return to the relationship



Safety Planning Action Examples

General

- Consider physical exit/escape options (e.g., vehicle, classroom, home)
- Alter schedules and routes
- Cease communication with Respondent
- Inform support system
- Notify school resource officer (SRO), campus security, and/or police
- Secure an emergency protective order
- Seek victim services assistance

Workplace/School Specific

- Inform coaches, teachers, counselors, supervisor, or other key administrators
- Provide photo to school resource officer (SRO) or other safety personnel
- Remove FERPA directory information
- Request supportive measures
- Use safety escorts while on school property
- Change workflow protocols

Safety Planning Action Examples (cont.)

Online

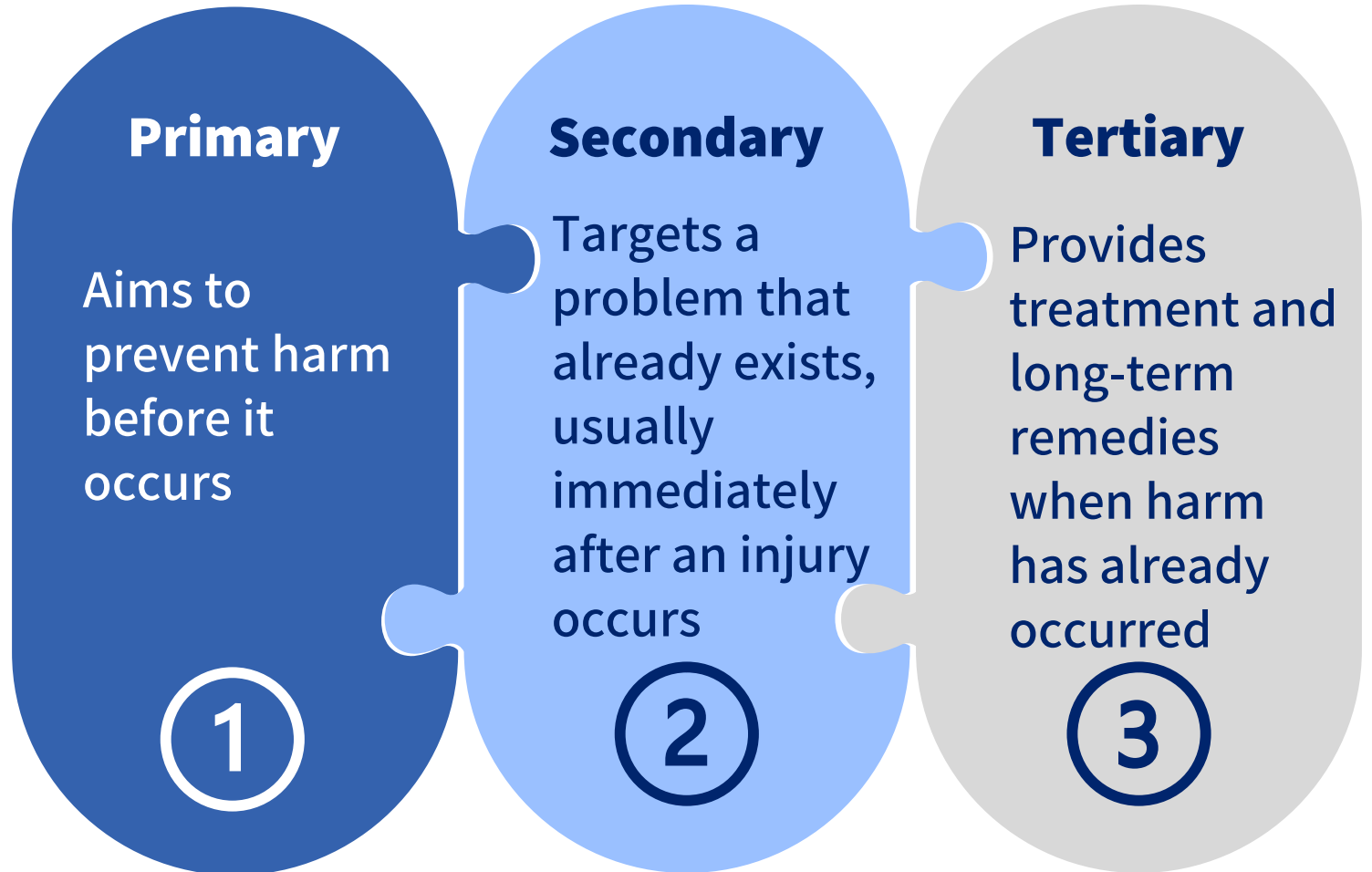
- Change passwords and answers to security questions
- Update privacy settings
- Implement multifactor verifications options
- Disable location sharing/tracking
- Set up fraud alerts with credit bureaus
- Acquire new devices

Prevention Education

What is Prevention?

An integrated and collaborative approach to addressing multiple areas of wellness that is:

- Evidence-based
- Multi-layered
- Directed at individual, community, and environmental levels



Prevention Education Recommendations

- Digital Citizenship
- Digital Consent
- Digital Safety
- Healthy Relationship
- Bystander Empowerment



Prevention Programming

- Programs tailored to each school/district and its populations
- Ongoing prevention and awareness campaigns
 - Responsive to community needs
 - Tailored to be culturally relevant and inclusive
- Direct programming to all students and employees
- Provide risk reduction information
 - Increase bystander action
 - Increase empowerment for victims



Association of
Title IX Administrators

Questions?



**ALL ATIXA PROPRIETARY TRAINING MATERIALS ARE COVERED BY
THE FOLLOWING LIMITED LICENSE AND COPYRIGHT.**

By purchasing, receiving, and/or using ATIXA materials, you agree to accept this limited license and become a licensee of proprietary and copyrighted ATIXA-owned materials. The licensee accepts all terms and conditions of this license and agrees to abide by all provisions. No other rights are provided, and all other rights are reserved. These materials are proprietary and are licensed to the licensee only, for their use. This license permits the licensee to use the materials personally and/or internally to the licensee's organization for training purposes only.

If these materials are used to train Title IX personnel, they are subject to 34 C.F.R. Part 106. If you have lawfully obtained ATIXA materials by registering for ATIXA training, you are licensed to use the materials provided for that training.

34 C.F.R. 106.45(b)(10) (2020 Regulations) requires all training materials to be publicly posted on a Recipient's website. Licensees subject to the 2020 Title IX Regulations may download and post a PDF version of training materials for their completed training to their organizational website to comply with federal regulations. ATIXA will provide licensees with a link to their materials. That link, or links to the materials on that page only, may be posted to the licensee's website for purposes of permitting public access to the materials for review/inspection only.

You are not authorized to copy or adapt these materials without ATIXA's explicit written permission. No one may remove this license language from any version of ATIXA materials. Should any non-licensee post these materials to a public website, ATIXA will send a letter instructing the licensee to immediately remove the content from the public website upon penalty of copyright violation. These materials may not be used for any commercial purpose except by ATIXA.