GUIDELINES FOR RESPONDING TO DIGITAL THREATS

If Threat is Imminent, call 911

What to do if:

IDENTITY OF THE AUTHOR IS KNOWN

1. Activate Threat Assessment Team and inform Law Enforcement

2. Assess the language of the threat for plausibility and specificity? (details, means, justification, target and site selection) – The Lower the Data, The Lower the Risk

3. Ensure the whereabouts of any person of concern if known and target(s) and address any immediate risk factors. If necessary, appropriately detain or monitor any person of concern and do not allow them access to their digital devices, coat, backpack, or locker

4. Remember to distinguish between assessing the threat versus assessing the threat maker (it is one thing to make a threat but another to be engaging in behaviors consistent with the threat)

***Remember:* Keep target(s) informed and provide information to staff, students, and parents as necessary as it helps lower the anxiety**

Check All (Where Applicable) for any evidence of threat-related items:

- □ **Backpack**
- □ **Desk(s)**
- □ **Vehicle (visual check)**
- □ **School Assignments**
- □ **Writings, Drawings, Artworks, etc.**
- □ **Co-Conspirators**
- □ **School Computers**
- □ **The Person**
- □ **Online Journals (School)**
- □ **All Digital Devices**

□ **Determine if any person of concern has access to weapon(s) (<u>If there is any evidence of accessing means to carry out a threat, exigent circumstances may exist to remove possible access to the means at various known locations)</u>**

5. Document and record threat (screenshot + download or save photos or videos)

6. Check Behavioral and Digital Baseline of the Threat Maker: Is this new behavior or are we just finding out about it now? If this is an established baseline, the initial level of risk diminishes but still requires behavioral management/modification

- Cross reference usernames
    - ○ Search for exact usernames within Facebook, Twitter, Instagram, and YouTube.
    - ○ Google search username to cross reference
- Google search for “full legal name” using Quotations
    - ○ Do the same for the given name or and any nickname(s) of possible authors of the threat

7. Verification check
    - ○ Any text – google in quotations to check for imitator language
    - ○ If Image – Reverse Image Search, Metadata check (is this image stock or unique, recent or old)

8. Has the threat maker engaged in behaviors that are consistent with the threat? Any known planning, research et al. (Interviews using open ended questions with peers should be considered, check all accessed school computer search histories for that individual)

9. When possible, interview the person of concern after initial data (from locker checks, interviews with the individual who reported the threat, checking with police for prior police contacts) have been collected. This will help to avoid a “uni-dimensional assessment" and provide the interviewer(s) with data to develop case-specific hypotheses and verbatim questions that can be asked in a strategic Threat Assessment interview to test the hypotheses. The interview with the known Threat Maker is often the most powerful intervention that will take place

Note: Law enforcement should initiate preservation order to social media platform if investigation proceeds.

https://www.search.org/resources/isp-list/

IDENTITY OF THE AUTHOR IS UNKNOWN

(Although unauthored threats may be credible in the world of global and domestic terrorism, in the field of school-based child and adolescent threat assessment, the lack of ownership or authorship of the threat generally denotes a lack of commitment)

Nevertheless, there are steps that should be followed

- Assess the unauthored threat
- Attempt to identify the threat maker
- Avoid or minimize the crisis/trauma response

1. Activate Threat Assessment Team and inform Law Enforcement

2. Assess the language of the threat for plausibility and specificity? (details, means, justification, target and site selection) – The Lower the Data, The Lower the Risk

3. Document and record threat (screenshot + download or save photos or videos)

4. What is the username attached to the threat? Note: when dealing with Snapchat, make sure you find the username, which is different from the vanity name.

- Cross reference usernames
  - Search for exact usernames within Facebook, Twitter, Instagram, and YouTube.
  - Google search username to cross reference
- Verification check
  - Any text – google in quotations to check for imitator language
  - If Image – Reverse Image Search, Metadata check (is this image stock or unique, recent or old)
- Identify others who need to be looked at / interviewed (Targets of the threat, individuals who would have perceived grievances)
  - Who shared the threat with the school? (Possibility of cry for help and sometimes the one who found the threat was the actual threat maker)

Note: Law enforcement should initiate preservation order to social media platform if investigation proceeds.

https://www.search.org/resources/isp-list/