BEST PRACTICE THREAT ASSESSMENT RECOMMENDATIONS FOR ALL SCHOOLS

From the Review of Psychological Safety and Threat Assessment Issues Related to the Arapahoe High School Shooting

Kanan, L., Nicoletti, J., Garrido, S. & Dvoskina, M., 2016

While most schools throughout Colorado and the country have been using a threat assessment process for years, this arbitration allowed the reviewers to look into specific implementation of the process through an examination of a select sample in one district and one school. The following best practice recommendations are made after review of information provided in this arbitration and are provided for ***all schools*** regarding the process, training, intervention planning and documentation of threat assessments in schools. All school districts and schools are encouraged to use the lessons learned and the information provided in this report to review their process, training and documentation of threat assessments and interventions for threat management.

Best Practice Recommendations for School Threat Assessment Process

1. One of the key elements in identifying a student in crisis or interrupting a potential school attack situation is *early detection*. The foundation for the threat assessment process involves raising awareness for detection of potential behaviors of concern, and about the timely reporting of those concerns. Awareness training must occur across school employee groups, students, parents, and others in the community. Multiple reporting methods for concerns are encouraged, as long as the vortex for information is established. See Section II of this report.

2. Each district is encouraged to review the training and experience of its administrators, mental health personnel, and others who might be members of a threat assessment team, to determine if the multi-disciplinary site-based 3-person threat assessment team model, as recommended by the CSSRC, can be implemented at their schools. Any gaps should be remediated.

3. Given the potential difficulty of assuring the training, and in some cases, the limited experience of site based administrators and mental health personnel, a designated district level subject matter expert or review team is recommended to be available for review, consultation, training, and participation in difficult cases, as needed.

4. The process should be consistent between a district level review team and school based threat assessment teams. The process should also be consistent across schools in each district.

5. The vortex for information reporting and consolidation should be established at each school. It is considered best practice if the vortex is a team, to reduce unilateral decision-making regarding the significance of behavioral data and threat assessment.

6. An outline of the key considerations in the process:

    a. Securing safety should be a priority.
    b. Notifications about the need for a threat assessment should occur and the threat assessment team should be convened.
    c. Information should be obtained from a variety of sources, including:
        - Searches of the person, as appropriate,
        - Searches of social media,
        - Reviews of school and other available records,
        - Information and observations from teachers or others at the school who know the student, and
        - Information from community treatment providers or other agencies providing intervention to the student.
    d. Special Education considerations should be reviewed and appropriate staff included in the process.
    e. Interviews should be conducted with the student of concern, parents of the student of concern, and witnesses (if relevant). This is best done *outside* of a meeting and should be conducted prior to the meeting where a plan is developed.
    f. All data should be reported in behavioral terms, when possible, and all data should be considered and evaluated.
    g. Organization and analysis of the information should occur.
    h. Decision-making should take place regarding the seriousness of the behavior by reviewing all the data sources. The foundation for the level of risk should be based on all the behaviors over time and the detail for the determination of risk should be recorded. Decision-making can be assisted by a system for behavior analysis and coding (Nicoletti model) and the Secret Service 11 Key Questions.
    i. Appropriate action and intervention planning (countermeasures) should be commensurate with level of concern.
    j. Identify strengths or relationships that can be developed, include specific steps of plan, details of monitoring, and people responsible for the action items (including the parent and student).
    k. Monitoring of student and review of the plan should be clear – Identify personnel who are the points of contact and establish a firm date for review of the effectiveness of the plan.
    l. A documentation form should be completed, in detail, with the foundation for the level of risk. Records should be maintained, as directed by the district.
    m. Review the effectiveness of the plan, student progress and document the follow up review meeting.

7. It is recommended that someone with experience and expertise at the central district office level and/or a district level team review the assessment and the action and intervention plan.

8. Central district record keeping should also be maintained. Cases reviewed by the threat assessment team at the school and district should be classified according to some follow up system such as:
    a. Currently active and under review
    b. Active with proactive monitoring of behavior and countermeasures
    c. Inactive with reactive monitoring, as needed.

Best Practice Recommendations for Training School Employees in Threat Assessment

1. All school employee groups should be trained for awareness of violence or concerning behavior and the importance of timely reporting.
    a. All students should also be trained about the importance of reporting.
    b. Parents should also be educated and reminded about the importance of reporting behaviors of concern, for the safety of their child and the safety of others.
    c. Schools must continue efforts to partner with parents for early intervention for kids exhibiting concerning behaviors.
    d. Multiple methods of reporting are encouraged, as long as the vortex for information is established and used.

2. All school district employees acting as part of a threat assessment team should be trained, including administrators. Updated training should be required at regular intervals (every 2-3 years). Attendance at trainings should be documented.

3. Law enforcement officers (SROs) acting as part of a school based threat assessment team should also participate in the district threat assessment training process or similar training.

4. When possible, teams should train or practice together. Much as schools are encouraged to drill and practice other types of emergency response procedures, threat assessment teams can also benefit from case practice.

5. Face-to-face training should always include review of any topics that are covered in handouts, support, or resource documents. Any supporting or resource documents provided in training should also be available on the district intranet.

6. Sufficient time must be dedicated to training on the important topic of threat assessment. Covering many related topics in one training session may be efficient and help to make connections of learning for staff, but this and other safety topics need dedicated training time. School and district leadership must support that training.

7. Best practice threat assessment training should include:

    a. Information content about the history of school related violence incidents and lessons learned.
    b. Clarity about ***when*** to do a threat assessment as stated in district information and policy.
    c. Clarity about the composition of a Threat Assessment Team, including attendance by a Special Education representative, if the student has an identified disability. The CSSRC (2010-2015) has recommended at least three trained members to a team.
    d. Six principles of threat assessment from the Secret Service recommendations (Fein, et al., 2002, 2004) to remind participants of the need for a skeptical mindset, basing information on facts, using integrated systems.
    e. Training and *emphasis* on relevant FERPA exceptions to confidentiality, as misperceptions still exist regarding this law and relevant exceptions (CSSRC, 2010-2015).
    f. Training for awareness of and *appropriate use* of warning sign indicators (Dwyer et al., 1998; CSSRC, 2010-2015; and others). These warning signs are for awareness of troubled students, and not necessarily students who are dangerous or pose a risk for violence. They should not be used as a checklist for violence as they not all equal in importance or as indicators (Dwyer et al., 1998; Cornell, 2014).
    g. Ten Key Findings from the Safe School Initiative (Fein, et al., 2002), as this information still applies, and can be useful in awareness training. These findings relate to information that should be questioned during a threat assessment process.
    h. Teach information for awareness of avenger violence (Nicoletti, 2013, 2014)
    i. Teach and give examples of how to evaluate written material (Kanan, 2010, 2011, 2013).
    j. Teach how to identify each type of threat for correct coding of behaviors (direct v. indirect, conditional, veiled, etc.) (O'Toole, 2000, Nicoletti, 2010).
    k. With regard to the "Access to Weapons" question, it is recommended that those completing these forms be trained to only mark "none known" after taking reasonable steps to ascertain the information. Document the attempt to gather information related to an armament.
        - Training should specify that both the student and their guardian should be asked directly if there are weapons in the home, if the student has access to weapons, and if they have had training. Specific responses should be noted.
    l. Train for evaluation of materials obtained. If the form directs the decision to assign a category for level of concern, examples and explanation should be provided.
    m. Teach about the identification and coding of behavior as "normal", "boundary probing" "attack related" or "attack" for use in determining level of concern. (Nicoletti, et al., 2010; Nicoletti & Spencer-Thomas, 2002).
    n. Use of the 11 Key Questions for the Secret Service should be reviewed and explained.
    o. Teach how to create effective intervention plans commensurate with the level of concern and provide suggestions for monitoring.

- Examples of effective intervention planning (countermeasures) should be provided. All students who engage in behavior that prompts a threat assessment should be monitored over time.

p. Train for each step of the district process, in addition to reviewing the form.
q. Teams should use case studies for tabletop practice in threat assessment.
r. Participants in trainings should be asked to complete a short evaluation to assess the effectiveness of the training, the presentation materials and format and to provide suggestions for future training. This will help assess which topics may need more information or additional training.

Best Practices Recommendations in Documentation of Threat Assessment and the Intervention Plan

1. All school district documentation forms should be reviewed to assure the form helps to guide less experienced school personnel through the district's process of threat assessment.

2. All school district Threat Assessment documentation forms should be reviewed for single prompts and contain sufficient additional space after each prompt for addition of clarification and/or evidence of the box checked.

3. A section for all the recommended data sources to be used in the assessment should be included.
    a. As mentioned in the process above, a search of social media activity *should be included as standard practice* as part of threat assessment process. Social media should consistently be searched and screenshots of any concerning posts, pictures, quotes, etc. should be included in documentation. Students can be asked to show their social media directly, parents should be involved, and law enforcement consulted, as needed. Consultation with school district attorneys can provide more guidance on reasonable suspicion in this type of search.

4. Documentation forms need to include a step to *evaluate available information* before any decision-making and intervention planning.
    a. Careful examination of behaviors and coding using the concepts of "normal", "boundary probing", "attack-related", and "attack planning" are useful for evaluation.
    b. Available guidance for school threat assessment continues to advocate for the use of the Secret Service 11 Key Questions as part of a threat assessment form and process in schools (CSSRC, 2015).

5. The intervention or action plan developed as part of a threat assessment *should be detailed, with appropriate steps, persons responsible to follow-up, and a date established for review of the plan* before the meeting is concluded.

6. All threat assessments should have intervention or action planning, *including monitoring of the student*. More examples of items to be used and blanks for other interventions the school-based team may create could be added to documentation forms.
    a. A Point of Contact (POC) should be identified and assigned to any student requiring a threat assessment and whenever possible, the POC would ideally be a school psychologist or other mental health staff member uniquely qualified to provide ongoing behavioral assessment and monitoring.
    b. Initially, a student that has engaged in a behavior requiring the completion of a threat assessment should be required to complete daily or weekly check-ins to assess their willingness and ability to comply with limit setting. Some suggestions for check-ins should be provided.
    c. There should be specificity to the check-in with students. Specify if the backpack, notebooks, locker, or social media pages will be checked or if check-in consists of verbal confirmation that things are going well. Document the check-in and specify what will happen if a student misses a check-in.

7. If the student does not comply with the required check-in or action steps (countermeasures), this may indicate a higher risk, as the student is demonstrating they are choosing to disregard rules or is incapable of controlling his or her impulses.

Key Findings and Recommendations From the Trend Analysis and Specific Case Review

1. Faculty and staff need to be trained on a standard protocol for detecting and reporting concerning behaviors as recommended in Section II of this report.

2. Students also need to receive training to notice concerning behavior ("what to look for") and how to report concerns, as in Section II.

3. There should be a variety of options for reporting concerns, such as: Safe2Tell, the district safety and security number, notifying the school administration, the school resource officer, counselor, school psychologist, teachers, parents, or others. However, *all of these options need to filter to the centralized vortex.*

4. Unilateral risk assessment should be avoided. *If you see something or hear something, say something*, and always consult with others to avoid unilateral assessments.

5. Data should be collected from multiple sources within and outside of the school, including from parents and caregivers, mental health professionals, and social media sources.

6. Concerning behaviors need to be appropriately documented *in behavioral terms* that make it clear what specifically was said or done that was of concern. Vague statements such as "he was awkward" or "his statement's were bizarre" should be avoided. Record

specific language use and save concerning writings or drawings for a record of *exact content.*

7. Threat assessment forms should be standardized and guide personnel, especially less experienced ones through the process of data gathering, consideration of risk, and the creation of an intervention plan. Behavior must be looked at over time. A specific review date should be established to review the effectiveness of the plan.

8. Threat assessment team members should avoid diagnosing emotions and *focus on the behavioral indicators.*

9. Any concerning behavior should be met with an intervention (countermeasure), and each countermeasure should be *monitored for effectiveness*. Again, reviewing behavior over time and the effectiveness of the countermeasures over time can be helpful to determine a pattern.

10. Cases reviewed by the threat assessment team at the school and district should be classified according to some follow up system such as:
    a. Currently active and under review
    b. Active with proactive monitoring of behavior and countermeasures
    c. Inactive with reactive monitoring, as needed.

For other prevention best practice recommendations from the report, go to: http://www.littletonpublicschools.net/sites/default/files/Kanan%20et%20al.%20AHS%20Report%202016.pdf.