

NaCTSO Guidance Note 8/2016

Advice to Leaders of Schools and other Educational Establishments for Reviewing Protective Security – Including Bomb Threats

Following a series of malicious hoax communications to schools across the UK, which are not being investigated as terrorism related offences, it is important that you are alert, but not alarmed. This is an opportunity for you to review your security plans to confirm that the arrangements you should already have in place are still current and have been tested to ensure staff and students are prepared and confident.

Consider what steps you could take to:-

- a) reassure your staff, students and parents
- b) review and implement proportionate protect and prepare security planning

1. Bomb threats: Procedures for handling bomb threats.

The vast majority of bomb threats are hoaxes designed to cause alarm and disruption. As well as the rare instances of valid bomb threats, terrorists may also make hoax bomb threat calls to intimidate the public, businesses and communities, to draw attention to their cause and to mislead police. While many bomb threats involve a person-to-person phone call, an increasing number are sent electronically using email or social media applications. No matter how ridiculous or implausible the threat may seem, all such communications are a crime and should be reported to the police by dialling 999. It is important that potential recipients – either victims or third-parties used to pass the message - have plans that include how the information is recorded, acted upon and passed to police.

1.1 The bomb threat message.

Bomb threats containing accurate and precise information, and received well in advance of an actual attack, are exceptionally rare occurrences. Precise motives for hoaxing are difficult to determine but may include revenge, extortion, a desire to impress, or a combination of these and other less understandable motives. In the vast majority of cases are hoax and the intent is to socially engineer, provoke a response, cause disruption or inconvenience the victim.

1.2 Communication of the threat.

A bomb threat can be communicated in a number of different ways. The threat is likely to be made in person over the telephone; however, it may also be a recorded message, communicated in written form, delivered face-to-face or increasingly, sent electronically via email or a social media

Protect yourself your staff your business and your community.

application e.g. Twitter or Instagram. It should also be noted that a threat may be communicated via a third-party, i.e. a person or organisation unrelated to the intended victim.

1.3 What you should do if you receive a bomb threat communication.

Any member of staff with a direct telephone line, mobile phone, computer or tablet etc., could conceivably receive a bomb threat. Such staff should, therefore, understand the actions required of them as the potential first response to a threat call.

If you receive a **telephone threat** you should:

- stay calm and listen carefully
- have immediate access to a checklist on key information that should be recorded (see bomb threat checklist - attached)
- if practical, keep the caller talking and alert a colleague to dial 999
- if displayed on your phone, note the number of the caller, otherwise, dial 1471 to obtain the number once the call has ended
- know who within your organisation to contact upon receipt of the threat, e.g. building security/senior manager
- if the threat is a recorded message write down as much detail as possible
- If the threat is received via text message do not reply to, forward or delete the message. Note the number of the sender and follow police advice

If the threat is delivered **face-to-face**:

- try to retain as many distinguishing characteristics of the threat-maker as possible

If discovered in a **written note, letter or as graffiti**:

- treat as police evidence and stop other people touching the item

If the threat is received via **email or social media application**:

- do not reply to, forward or delete the message
- note the sender's email address or username/user ID for social media applications
- preserve all web log files for your organisations to help the police investigation (as a guide, 7 days prior to the threat message and 48 hours after)

REMEMBER **Dial 999** and follow police advice. Seek advice from the venue security/operations manager as soon as possible.

1.4 The Credibility of Bomb Threats.

Evaluating the credibility of a threat is a critical task, particularly if the attack being threatened is imminent. This is a tactic used to place additional pressure on decision makers. When specific intelligence is known to police, advice will be issued accordingly; however, in the absence of information, it will be necessary to consider a number of factors-

- is the threat part of a series? If so, what has happened elsewhere or previously?
- can the location of the claimed bomb(s) be known with precision? If so, is a bomb visible at the location identified?

Protect yourself your staff your business and your community.

- considering the hoaxer's desire to influence behaviour, is there any reason to believe their words?
- if the threat is imprecise, could an external evacuation inadvertently move people closer to the hazard?

2. Evacuation considerations.

Responsibility for the initial action taken at a venue subject to a bomb threat sits with the establishment, not police. However all bomb threats should be reported to the police and their advice followed accordingly. Venue options include:-

2.1 External evacuation.

Leaving the venue will be appropriate when it has been directed by police and/or it is reasonable to assume the threat is credible and evacuation will move people towards a safer location. Appoint people, familiar with evacuation points and assembly (rendezvous) points, to act as marshals and assist with this procedure. At least two assembly points should be identified in opposing directions, and at least 500 metres from the suspicious item, incident or location. Where possible the assembly point should not be a car park. You may wish to seek specialist advice, which can help to identify suitable assembly points and alternative options as part of your planning. Where there are large numbers of people consider a phased evacuation, initially from the immediate area of the device. This will avoid unnecessary alarm and promote a safer evacuation. Each venue is unique and should plan and exercise for different threat scenarios.

The police will establish cordons depending upon the size of an identified suspect device. Always follow police directions and avoid assembly close to a police cordon.

Minimum police cordon distances are:-

100m – small items e.g. rucksacks or briefcases

200m – medium items e.g. suitcases, wheelie bins or cars

400m – larger items e.g. vans or lorries

2.2 Internal or inwards evacuation (invacuation).

Staying in your venue but moving people away from external windows/walls and is relevant when it is known that a bomb is not within or immediately adjacent to your building. Also consider that if the location of the device is unknown, is an evacuation necessary. If a suspect device is outside your building it may put people in danger if the evacuation route takes them past the device. A safer alternative maybe the use of internal protected spaces. Inwards evacuation needs significant pre-planning and may benefit from expert advice to assist in identifying an internal safe area within your building.

2.3 No action. This will be reasonable and proportionate if, after the evaluation by the venue, the threat is deemed implausible or a hoax. Police may provide additional advice and guidance. A proportionate search of the venue should be considered.

Remember: it is vital that regular drills are carried out to ensure all are familiar with bomb threat procedures, routes and rendezvous points. Disabled staff should have personal evacuation plans and

Protect yourself your staff your business and your community.

be individually briefed on their evacuation procedures. Similarly all visitors should be briefed on evacuation procedures and quickly identified and assisted in the event of a threat.

Familiarising through testing and exercising will increase the likelihood of an effective response to an evacuation. Evacuation procedures should also put adequate steps in place to ensure no one else enters the area once an evacuation has been initiated.

<http://www.cpni.gov.uk/Security-Planning/Business-continuity-plan/Evacuation-planning/>

3. Search Considerations.

Regular searches of your establishment, proportionate to the risks faced by an organisation, will enhance a good security culture and reduce the risk of a suspicious item being placed or remaining unnoticed for long periods. To that end:-

- ensure plans are in place to carry out an effective search in response to a bomb threat
- identify who in your venue will coordinate and take responsibility for conducting searches
- initiate a search by messaging over a public address system (coded messages avoid unnecessary disruption and alarm), by text message, personal radio or by telephone cascade
- divide your venue into areas of a manageable size for 1 or 2 searchers. Ideally staff should follow a search plan and search in pairs to ensure nothing is missed
- ensure those conducting searches are familiar with their areas of responsibility. Those who work regularly in an area are best placed to spot unusual or suspicious items
- focus on areas that are open to the public; enclosed areas (e.g. cloakrooms, stairs, corridors, lifts etc.) evacuation routes and assembly points; car parks, other external areas such as goods or loading bays
- develop appropriate techniques for staff to be able to routinely search public areas without alarming any visitors or customers present
- under no circumstances should a suspicious item found during a search be touched or moved in any way. Immediately start evacuation and dial 999
- ensure all visitors know who to report a suspicious item to and have the confidence to report suspicious behaviour

<http://www.cpni.gov.uk/Security-Planning/Business-continuity-plan/Search-premises/>

4. Media and Communication.

Avoid revealing details about specific incidents to the media or through social media without prior consultation with police. Do not provide or give details of the threat or the decision making process relating to evacuation, internal evacuation, or taking no action.

Releasing details of the circumstances may:-

- be the objective of the hoaxer, providing them with a perceived credibility
- cause unnecessary alarm to others
- be used by those planning to target other venues
- illicit copycat incidents
- impact upon a subsequent investigation

Protect yourself your staff your business and your community.

5. Firearms and Weapons Attacks. RUN HIDE TELL

<https://www.gov.uk/government/publications/recognising-the-terrorist-threat/recognising-the-terrorist-threat>

<https://www.gov.uk/government/publications/stay-safe-film>

6. Dynamic Lockdown Guidance.

<https://www.gov.uk/government/publications/developing-dynamic-lockdown-procedures>

7. Staff Awareness and Security Culture. Have you briefed your staff on how they can recognise suspicious activity? Consider an employee vigilance campaign

<http://www.cpni.gov.uk/advice/Personnel-security1/Employee-vigilance/>

Are all aware of the procedures to follow should they suspect suspicious behaviour? (Anti-Terrorist Hotline 0800 789 321) If you require an immediate response call 999

Preparedness: Are your first aid kits and emergency grab bags checked regularly, complete and accessible?

8. Physical Security. Have you checked CCTV systems? Are they all working correctly? Are the date/time stamps accurate?

<http://www.cpni.gov.uk/advice/Physical-security/CCTV/>

9. Mail Handling. A threat may still exist from items delivered to your establishment by hand or by post. Are staff familiar with indicators for suspicious deliveries?

<http://www.cpni.gov.uk/advice/Physical-security/Screening/Mail-and-deliveries/>

10. Security Guidance for Educational Establishments.

<https://www.gov.uk/government/publications/counter-terrorism-protective-security-advice-for-higher-and-further-education>

11. Emergency Planning and Response Advice.

<https://www.gov.uk/guidance/emergencies-and-severe-weather-schools-and-early-years-settings>

There is no change to the UK terrorist threat level, which remains at **SEVERE**; meaning an attack is highly likely.

Protect yourself your staff your business and your community.