Department for Education

Protective security and preparedness for education settings

April 2024

Contents

Summary

This non-statutory guidance provides advice to help educational settings to become better prepared for and able to respond to terrorism and other major incidents. It sets out practical steps to keep learners and staff safe in the event of an incident through simple and cost-effective methods.

The guidance is aimed at those working in settings who have existing responsibilities for emergency planning and response and site security and staff new to concepts of protective security and preparedness. It is recommended that all staff read this guidance to ensure all are able to identify security vulnerabilities, suspicious activity and respond when there is an incident.

For the purpose of this guidance, educational settings cover settings from Early Years, all schools, Higher and Further Education (including colleges, Sixth Form Colleges and Independent Training Providers), and alternative provisions (including special schools and children's social care settings).

How to use this guidance?

This guidance adapts principles from the National Counter-Terrorism Security Office (NaCTSO) into more sector-specific advice and offers interactive resources to help education settings embed these principles.

It helps with preparing and drafting plans and procedures to be better able to deal with incidents at or near an education setting. For settings that already have protective security and preparedness plans, or critical incident plans this guidance will assist you to review your approach.

Templates, examples, and case studies are available for you to save in an editable format and adapt for your setting to embed good practice.

The template 'protective security and preparedness self-assessment' (found separately in Annex D) is the overarching tool to help you translate the main principles in this guidance into the policies and plans that will work for your setting. If you already have established plans in place, you should use the suggestions in this template to review your approach, rather than creating an additional document. There are four templates available to use and edit within Annex D, which can be found on the same page as this guidance on GOV.UK.

ProtectUK can support you in developing these plans or reviewing plans you may already have. It is a free and authoritative resource to use in developing plans.

You can refer to the glossary section at any time for an explanation of the terminology used in this guidance.

Overview

- settings should make simple plans to improve protective security awareness and preparedness that can deter terrorists and other security threats looking for a target and help keep learners, staff and visitors safe.
- a Security Lead should be appointed to develop and maintain policies and plans which promote a good security culture and deters someone intending to cause harm from targeting your setting. During a live incident, the Security Lead may also become the 'Incident Lead' who will make effective decisions under pressure to get people to safety. However, all staff will need to play a vital role in responding to an incident.
- settings should consider what works best for learners and staff with Special Educational Needs and Disabilities (SEND) to ensure that policies, plans and procedures are inclusive and accessible.
- See, Check and Notify (SCaN) helps identify suspicious activity and deter and detect someone intending to cause harm targeting which can be easily applied to all settings.
- settings can also use the HOT protocol to identify suspicious items.
- settings should create a 'Bomb threat checklist' in preparedness for a live incident. All staff should be familiar with the processes.
- all staff should familiarise themselves with RUN HIDE TELL to ensure they can immediately respond to live incidents and make adjustments for those with SEND if required.
- educational settings should consider three response options to a live incident: Lockdown, Invacuation and Evacuation.
- Personal Emergency Evacuation Plans (PEEPs) should be in place for those required. These plans should also be adjusted to consider the impact of disability and alternative arrangements for learners with SEND.
- settings should consider compiling a grab kit comprising of key items that can assist during an incident; this is particularly helpful for learners with SEND.

Introduction

Settings can make simple plans to improve protective security awareness and preparedness that can:

- deter terrorists looking for a target.
- support settings to mitigate against a wider range of threats such as anti-social behaviour, dangerous animals on site, and other criminality; and
- help keep learners, staff and visitors stay safe.

Proportionate, low or no-cost changes can help keep people safer during any type of security incident without causing additional burden on the workforce.

What does good look like?

Settings should have plans in place to reduce the risk of terrorist incidents and other incidents by making it difficult for someone intending to cause harm to target their sites. All staff should understand the actions that they can take to be part of a good security culture that reduces the risk of an incident occurring.

Settings should have plans in place to respond effectively to different types of incidents. If an incident does arise, staff should be able to draw on their knowledge from plans and make good, informed judgements about how to keep themselves and others safe.

Settings should test their plans to make sure they are suitable and effective, for any live testing such as practice drills, consideration must be taken around individual trauma particularly around those learners who have previously been affected by incidents.

Staff roles in protective security and preparedness

It is good practice to have clear roles and responsibilities for protective security and preparedness. Your setting may use different terms from the standard job titles set out below and you may prefer to use other terms.

You should have a competent person or persons to lead in health and safety, and security. This may or may not be the same person and should either be a teacher, Headteacher or a designated Security Lead.

Teachers and Headteachers

Headteachers (and where delegated, deputies and assistants) have a contractual duty to promote the safety and well-being of learners and staff. Teachers have a similar duty to promote the safety and well-being of learners. Therefore, teachers or Headteachers may be expected to take on roles and responsibilities.

Security Leads

Responsible for coordinating and overseeing your setting's protective security and preparedness. All staff should know who the Security Lead is and focus on:

- developing, maintaining and updating policies and plans which promote a good security culture and deters someone intending to cause harm from targeting your setting.
- determining how staff should respond effectively to different types of incidents.
- ensuring that all staff members are aware of their roles and responsibilities in relation to protective security and preparedness, including ensuring that staff are appropriately trained.
- liaising with external agencies, such as police and emergency services, to ensure effective communication and collaboration.
- managing and delegating the response to an incident. The Security Lead will normally become the 'Incident Lead' however, settings should ensure one or two people are available to deputise during any absence.

Incident Leads

This role becomes active during an incident and should be responsible for, or should delegate the following responsibilities:

- leading the initial response to the incident within the setting.
- liaising with the police to incorporate their advice into an overall site response.

- making fast, clear decisions under pressure, to get people to safety.
- responding appropriately to any safety concerns, for instance people reported missing.
- communicating about the incident to parents and carers of those affected.
- leading any responses to interest on social media and in the mainstream media, if required.
- managing resources effectively, including consideration for the wellbeing of staff, learners and families affected.

All Staff including non-teaching staff

All members of staff have a role to play in your settings' security culture and preparedness. Staff responsibilities may include:

- participating in training and awareness programmes related to protective security and preparedness measures.
- being vigilant and reporting any suspicious activity to the Security Lead or appropriate authorities.
- supporting the Security Lead in implementing and maintaining the protective security and preparedness plan.
- being familiar with incident response plans, such as lockdown, invacuation and evacuation options, exit routes, methods of communicating in an incident, and compiling grab kits.
- providing additional support to those who are particularly vulnerable for instance, staff or learners with SEND.

During an incident, staff should:

- be prepared to call 999 unless they are certain that someone else has already called the emergency services (members of staff should not assume that someone else has called 999).
- keep track of the learners who they are with and report any concerns about the safety of any learners to the Incident Lead and/or police.
- escalate the incident to the security lead or to another senior member of staff, so that an Incident Lead can be delegated.
- be responsible for their own safety, but also be aware of the duty of care they owe to all learners within their setting.
- be aware of the incident response plan for the setting and undergo relevant incident response training.
- make dynamic decisions using their best judgement based on the information available to them.

- staff should advise any other adults on site how to respond, particularly visitors who are not aware of the incident response plans.

For Special schools and learners/staff with SEND:

- staff should consider what works best for learners and staff with SEND to ensure that they are not left feeling overwhelmed.
- to help learners keep calm, staff should role model calmness and make expectations about appropriate behaviour clear to learners depending on their age and disability.
- staff need to keep track of the learners who they are with and report any concerns about the safety of any learners to the Incident Lead and/or police.
- ensure the appropriate level of care should be taken for those learners with SEND: learners with SEND may find this process overwhelming or difficult to follow, settings should therefore consider having specific buddies/marshals to assist these learners.

Settings should already have fire marshals and first aiders in place. You should ensure that staff with these responsibilities receive sufficient incident training to perform these roles and are part of any testing and exercising.

Tailoring your plan to your setting

To determine what is appropriate for your learners, you should consider:

- who are your learners, and what specific needs do they have? How will SEND learners be affected? Is there anything that you need to do to tailor your plans so that these learners are kept safe?
- the best was to engage with your learners?
- how should you convey safety messages in a positive, reassuring way?

To determine who your learners are, and what specific needs they have:

- you should consider the type of activity, age, abilities, behaviours and mental health of the learners involved (including the reactions of learners with SEND).
- you should be aware of any learners who have experienced traumatic situations, for example having witnessed weapon attacks, having travelled from war zones, or been involved in terrorist incidents in the UK.
- you should consider how to emotionally support these learners in any safety protocols, for example giving them prior warning of the safety drills, allowing them to opt out, or allocating a specific adult to stay with them during the drill.

What do the various engagement activities involve?

There are a range of engagement activities to consider. Some will be more appropriate for your learners than others. Here are some suggestions, but you may also think of other options:

- you should discuss basic security messages and incident response plans as part of topics on personal safety or risk management in PSHE (Personal, Social, Health and Economic) education.
- you should encourage older learners to look out for suspicious items (using the HOT protocol).
- younger learners should be encouraged to tell their teacher if they see someone or something strange.
- some settings use coloured lanyards to indicate whether an adult is DBS (disclosure and barring service) checked, younger learners can also be good at spotting someone using a different colour to normal.
- drills should give learners the experience of practicing an incident response such as a lockdown, see further details below.

Involving learners in practice drills or exercises

As a general benchmark, it is relatively uncommon for security incident exercises or drills, such as lockdown drills, to involve primary school and Early Years learners. Instead, staff in primary schools and Early Years settings may hold drills for staff at a time when younger learners are not present.

It is more common for drills to involve learners of secondary school age and older. This experience works best as part of wider plan to share security awareness and incident response plans in an age-appropriate way.

You should consider how to best meet the needs of learners with special needs, those with Personal Emergency Evacuation Plans, and those who have previously experienced trauma that may be triggered by drills or exercises.

Learners with SEND

You should not exclude learners with SEND and you should build your drills with inclusivity and accessibility in mind. However, participating may be assessed following a risk assessment or case-by-case basis. This will enable the school to review their current plans and amend accordingly if required. For instance:

Example A

School A runs a practice lockdown drill, their current plans do not take into consideration Learner A who is a wheelchair user.

During the practice lockdown, staff and learners exit the setting from the rear into the nearby playing field. Learner A is unable to use their wheelchair as there is no accessible ramp.

School A then amends their plan to make reasonable adjustments for learners with physical disabilities, making their building more accessible.

Example B

School A runs a practice lockdown drill, their current plans do not include grab kits which include Learner A’s medication. This medication is essential for Learner A and it must be taken at the exact time.

During the practice lockdown, Learner A’s medication is not taken and if this were a live incident, the learners and staff would have no access to the room where the medication is located.

School A then amends their plans to include grab kits for learners particularly with SEND to ensure that their medication (and other essential items) stays with them at all times.

You should consider:

- can you make security drills feel equivalent to fire drills, so that learners have a familiar frame of reference to build on?
- should you give learners prior warning of drills and an opportunity to raise issues and worries with staff?
- should you allow learners to opt out, or allocating a specific adult to stay with them during the drill.
- consider learners with SEND in this process.

Building up to a drill in stages

One further education college took a staged approach to gradually build up to a full lockdown drill. This also built learners' knowledge and confidence of the process.

Stage 1: Programme of awareness - raising awareness on campus to inform and educate learners about counter terrorism preparedness.

Stage 2: First lockdown drill - provide warning of the drill by informing learners and staff of the date and time of the drill. At the drill, event marshals should overtly observe.

Stage 3: Second lockdown drill – this drill should have less detailed warning, with the exceptions of certain learners who may have suffered post-traumatic stress.

Stage 4: Third lockdown drill - surprise lockdown drill with no warning, with the exceptions of learners who may have suffered post-traumatic stress.

Any conversations about security procedures should be reassuring and those leading in drills and exercises should try to remain calm, speaking in a reassuring, assertive tone.

Staff should ensure that discussions and activities are conducted with sensitivity and awareness of the learner's comfort levels. Whilst drills and exercises should try and create realistic scenarios, it is important not shock or frighten learners. For example, drills, exercises and safety videos should not mimic behaviours of someone intending to cause harm (shouting, running, waving weapons), respondents (shouting, crying, panicking) or police officers (shouting, aggression, pointing weapons).

Discussions and drills should focus on safety procedures and avoid implying the motivations for a possible attack. The motivation of someone intending to cause harm is

irrelevant to the core safety messages about how to respond and should promote stereotypes or misconceptions about who the attacker may be.

Some incident preparation messages for learners, parents and carers.

Example 1: For learners and parents and carers

The chances of a terrorism incident (or other security incident) is low. Though we believe that it is extremely unlikely to happen at 'our educational setting' [Name of educational setting], we want to ensure that plans are in place to embed good practice across the site that keep us all safe, should there be an incident. This will involve practice drills so that learners and staff know what to do when an incident happens and embedding a detailed plan so that staff are aware of roles and responsibilities.

Example 2: For learners at the setting

If an incident is happening:

- stay calm.
- stay silent (we understand that this might be difficult for younger learners and/or those with SEND, that is why we encourage settings to practice drills)
- follow instructions straight away, from your teacher, other members of staff or the police.
    - for your safety, you may be asked to do things that are usually against the school rules. For example, to leave the building quickly, you might be asked to run in a corridor or climb through a window. To safely hide somewhere, you might be asked to go into a room that is usually out of bounds. During a drill or an incident, all these things are allowed if they are part of the instructions from a responsible adult.
- prioritise your safety: do not use your phone or other device for filming, taking photos, phone calls, messages, or social media. These are all distractions from your safety, and they may create noises.
- silence your devices (if they are not already turned off) - switch devices off or put them on airplane mode.
- you may see armed police (police officers with guns).
- you should treat all drills and exercises just like they are real incidents.

Impacts of live exercises and drills on your neighbours

A real incident may not be solely confined to one site and may have impacts in the wider neighbourhood; therefore, a realistic live exercise or drill of an incident response may need to involve the other educational settings and businesses nearby.

When considering how to involve nearby settings in your drill or live exercise you may need to test and practice how you would alert them of the incident taking place or evacuating to muster points on their site. Where possible you should try and involve neighbouring settings in the planning and testing of your exercises.

You should also consider whether to involve your governing body or academy trust local authority, or local police, to either take an active part in your practice drill or live exercise, or to help evaluate it.

Embedding this section to your plan:

- you should set out your staff roles using the template ‘protective security and preparedness plan
- when writing your plan, you may wish to consider creating action cards for staff to utilise in the event of an incident to remind them of the site policy and processes
- you should regularly test your plans. Practice drills will help test the response of staff and learners and identify where improvements can be made
- you should read the section, “Discussing protective security and preparedness in your education setting”, which includes further information about an armed police response during an incident

Embedding a security culture

Security is not just about obvious physical measures such as fences and CCTV. Security in settings can be improved in simple and subtle ways that have a significant impact. Most settings will already have an established culture relating to the prevention of harm, arising from health and safety, safeguarding and risk management work over many years. This provides a great starting point for developing counter terrorism practices into the existing security culture.

The National Protective Security Authority (NPSA), has produced guidance for settings about the concept of Security-Minded Communications. It focuses on preventing someone intending to cause harm from obtaining information that they would find useful, and how to use communications to deter from targeting your setting.

You should review this guidance and then return here to continue. Click to open the Security Minded Communications in a new tab.

How to respond to unusual and suspicious activity

Your setting should have existing safeguarding procedures in place; this means staff may already be aware of the need to approach someone behaving in an unusual manner. For example, taking photographs of learners in the playground, or unescorted visitors in the corridor.

See, Check and Notify (SCaN) aims to help businesses and organisations maximise safety and security using their existing resources. These principles can be applied to settings.

SEE - be vigilant for suspicious activity.

Suspicious activity occurs when you recognise actions that may indicate pre-operational planning associated with dishonest activity resulting in terrorism or crime. Suspicious activity occurs when you recognise actions that may include:

- someone trying to remain hidden or out of view.
- someone covertly or overtly taking photographs of security measures, such as CCTV, access controls, entrances and exits, or staff.
- a bag being left in a normally crowded area, or by an entrance/exit.
- someone attempting to gain entry to restricted areas.
- someone loitering in restricted or non-public areas.
- someone asking unusual questions.

A vehicle could also seem suspicious if:

- it is positioned in an unusual way (mounting a curb close to the entrance/exit or the side of a building).
- appears abandoned.
- contains passengers who are observing the setting and are not known to staff and do not appear to be dropping off or collecting anyone.
- contain items like petrol cans, flammable liquids or knives or weapons.
- be driving a number of times along the same route around the site.
- have window tints that restrict your ability to see inside the vehicle and its occupants.

Seeing a vehicle behaving suspiciously should prompt staff to consider if there have been any other suspicious activity around the site.

CHECK - Use the 'power of hello'.

The 'power of hello' is about approaching a person (if safe to do so), whose activity could be considered suspicious; this can disrupt potential criminal activity. It shows the individual that you have noticed them and are aware (vigilant) of activity being conducted in and around your setting.

NOTIFY - reporting suspicious activity.

If a person or vehicle is on site and you are suspicious about their intentions or activity, then you may need an immediate police response (dial 999 for the police).

It is beneficial for the person to be on site when the police are called. If the person has left the scene and the route, they took is unknown, or a significant period of time has elapsed since the incident, you should:

- contact the Anti-Terrorist Hotline on 0800 789321 or
- report the incident online or
- call 101

You can also report suspicious activity online, in confidence to the Action Counter Terrorism (ACT) website. Alternatively, the ProtectUK app brings together many different ways of reporting incidents.

How to respond to an unattended or suspicious item

One way that terrorists may operate is to place a bomb concealed inside any item including a package, bag, holdall or rucksack, then leave the area before the bomb detonates. It is important to note, that bombs can be found in places other than holdalls and rucksacks.

In a setting, unattended bags are common, and good housekeeping that keeps clutter to a minimum and setting tidy helps make suspicious items easier to identify. Having a good awareness of the characteristics that makes an item suspicious will mean that staff can take a proportionate approach when considering their local knowledge and the information available to them. The HOT protocol (Hidden, Obviously suspicious, Typical) helps to determine whether an item is suspicious.

Use the HOT protocol to judge whether an item seems suspicious, after considering all the information available to you and local context to the situation in each case.

To see how this should be implemented in educational settings, you should complete the Act for Education e-learning modules.

HOT protocol

Hidden?

- has the item been deliberately hidden, or has a deliberate attempt been made to conceal it from view?

Obviously suspicious?

- are there wires, circuit boards, batteries, tape, liquids or putty-like substances visible?
- has the item been found after seeing suspicious behaviour? Ask if anyone nearby has left the item or saw who did. You could use CCTV, if available

Typical of what you would expect to find in this location?

- consider whether unusual looking tools, devices or cables are likely to have been left innocently by others or maintenance staff working in the area
- does it look typical of what would be expected to be in that location?

Based upon what you can see, do you think the item poses an immediate threat to life?

If the item is assessed to be unattended rather than suspicious, carefully examine further and assess before applying lost property procedures.

Suspicious items represent a potential risk to life. Where an individual has identified a suspicious item, they may need to take immediate action to move people away and contact the police.

Assistance should be provided to cordon off an area. This is crucial for the safety of all staff and learners and is particularly important for vulnerable learners such as early years, primary aged and learners with SEND.

The 4 Cs protocol (Confirm, Clear, Control, Communicate) sets out how people can best respond to unattended items, once they have been assessed as suspicious.

If you believe the item is suspicious and represents a possible risk to life, then continue with the 4 Cs protocol (Confirm, Clear, Control and Communicate). These should all be considered concurrently.

Confirm – whether or not the item has suspicious characteristics.

- this is a critical part of the process and should be considered using all available information to hand before using the HOT protocol to judge whether an item seems suspicious.
- if you believe the item is suspicious and represents a possible risk to life, then consider the item as suspicious with relevant partners and continue with the 4 Cs protocol (Confirm, Clear, Control and Communicate). These should all be considered concurrently.

Clear – the immediate area.

- do not touch the item.
- take charge and move people away from the item.
- consider evacuation procedures to quickly alert people to clear the area and move to pre-arranged muster points based on the size and location of the item.

Control – access to the unsafe area.

- prevent others from approaching the unsafe area.
- keep eyewitnesses on hand so they can tell police what they saw and try to obtain the contact details of witnesses before they leave.

Communicate

- inform your senior staff and any security officers, explain why you consider the item suspicious.
- do not use radios or phones within 15 metres of the item, this is about the length of 3-4 cars.
- call 999 to alert the police.

You may want to consider asking parents and carers to look out for suspicious activity, utilise the ‘power of hello’ and share information about the HOT protocol with them to identify suspicious items to make them part of your setting’s security culture.

Bomb Threats

What is a bomb threat?

For the purposes of this guidance, a bomb threat is where an individual places an article or communicates information with the intention of inducing a person to believe that something is likely to explode or ignite causing harm within an educational setting.

Bomb threats containing accurate and precise information, and received well in advance of an actual attack, are rare occurrences. Most bomb threats are hoaxes designed to cause fear and disruption. Terrorists and others may make hoax bomb threat calls to intimidate the public, to draw attention to their cause and to mislead police.

A bomb threat may be communicated in different ways:

- phone call.
- recorded message, possibly using a text-to-speech synthesiser or a soundboard.
- communicated in written form.
- delivered face-to-face.
- sent by email or social media.
- via an independent third-party, i.e. a person or organisation unrelated to the intended victim and selected only to pass the message.

All bomb threat communications are a crime and should be reported to the police by dialling 999, no matter how ridiculous or implausible the threat may seem.

How to immediately respond to a bomb threat?

If the threat is made by phone or in person, try to keep the speaker talking to gather more details about the bomb, for example when they say it will go off, or their motives. Take in as much information as possible:

- can you remember or record the exact wording they use?
- what can you tell about the person making the bomb threat (e.g. accent, gender, background noises, visual appearance)?
- do you have information about their identity. For instance, what phone number, email address or user ID are they using?

If you can, grab your bomb threat checklist. It will help you remember what to do and observe, and to record details about the threat immediately. If you cannot use a bomb threat checklist, then you should still try to log as many details as you can about the threat. You should also:

- call the police on 999 as soon as possible, and share all details of the threat.

- (if you are receiving a bomb threat call, try to attract the attention of a colleague who should immediately dial 999).
- escalate the incident to the Security Lead or another senior member of staff who can best lead your setting's incident response, and relay any police advice to them.

Record and retain all evidence and make this available to the police. Ways of doing this include:

- If you received a threat on a landline, you should dial 1471 after the call to try to identify the phone number they used.
- Do not delete, reply or forward any emails, text or voice messages, this will prevent others from disturbing the evidence.
- Complete and retain your bomb threat checklist or other incident log.

The police may be able to advise on your response to the incident, including how to manage risks and keep people safe. However, the incident lead should consider the following:

- which exit/evacuation routes will be safe to use?
- context: is there anything that has happened before now that may be linked to this bomb threat, such as a pattern of previous threats or recent reports of suspicious behaviour, or could it be a last day of term prank? What extra information does the context give you about the credibility of this threat?
- is someone able to check recent CCTV footage? Would this give you useful additional information?

RUN HIDE TELL

All staff, including regular contractors such as cleaning and catering staff, need to be able to make informed choices when faced with a terrorist incident. Understanding and remembering the RUN HIDE TELL principles, combined with good knowledge of your site, its capabilities and your emergency procedures will help people respond dynamically to each unique incident.

Knowledgeable staff should guide less knowledgeable people, such as learners, visitors, any contractors, and any members of the public.

To introduce you to RUN HIDE TELL, watch this two minute video (opens in a new tab) and then return here to continue.

RUN

- if you can, locate the threat using sight and hearing.
- if there is a safe route, run.
- insist others go with you, but don't let their hesitation slow you down.
- don't waste time filming videos or collecting belongings.
- running to safety is your best option.

HIDE

- if you are unable to run, hide.
- if possible, lock yourself in a room with solid walls, barricade yourself in and move away from the door.
- find cover that can withstand threats such as a knife attack.
- you may need to use any hiding place that puts you out of sight of the attacker.
- be very quiet and still, silence your phone and turn it off vibrate. Avoid any noise or movement that will attract the attacker.
- stay hidden until you are rescued by identifiable police emergency responders.

The principles of HIDE are the same as what you need to do in a lockdown. HIDE is an individual response to a threat, whereas lockdown is an overall site response strategy, decided by the incident leader.

TELL

- call 999 only when you are completely safe to do so.
- listen carefully to the operator and give as much information as you can.
- if it is safe to do so, stop other people going towards the danger.

- can you also alert other staff in the building to the threat?

For learners and staff with SEND, it may be difficult to embed RUN HIDE TELL principles. Schools should therefore adjust the generic plan to consider the impact of disability and plan holding areas if necessary; this includes making alternative arrangements for learners with SEND.

To see how this should be implemented in education settings for 11-16 year olds, you should consider the Act for Youth teacher guidance and lesson plans.

Response options for your setting

This section explains what pre-planned incident response options you can embed across your educational setting to move learners, staff and visitors to a place of safety.

You need to plan for a number of different incident response options, so that staff can choose the most appropriate option for the particular circumstances of any incident that they face.

Option 1: Lockdown

A lockdown is about locking or barricading a room's doors and windows to delay or deter someone intending to cause harm from getting into an area. You should consider in advance to what extent you might be able to lock or barricade classrooms and other spaces in your setting during an incident, and whether additional door jamming, or lockdown devices are needed.

If a barricade cannot entirely prevent entry to a room, you may also need to identify spaces within that room where people could hide from someone intending to cause harm. You should turn off lights and close any blinds to prevent them seeing into the room. Keeping learners calm and quiet during a lockdown should reduce the risk of drawing attention.

In early years settings, primary schools or special schools, learners may be fearful of dark rooms, these settings should therefore consider dimming the lights instead and using ear defenders to assist learners to remain quiet.

The principles of what to do in a lockdown are the same as the HIDE part of RUN HIDE TELL. HIDE is part of an individual response to a threat. Lockdown is an incident response strategy for a site, decided by the Incident Lead.

To see how this should be implemented and test understanding you should complete the Act for Education e-learning modules.

Option 2: Invacuation

Invacuation is moving people inside a building to a place of relative safety.

Protected spaces are locations within your building(s) that have previously been identified as places of relative safety, where people can hide or shelter from threats. To protect from bomb attacks, protected spaces typically have substantial walls and offer low risk from flying glass from windows. It should be possible to lock or barricade the entrances/exits to the protected space. In planning protected spaces, you need to

consider how many people could safely be accommodated within each identified protected space.

Option 3: Evacuation

Evacuations are about moving people outside the building to protect from a threat in the building.

Types of evacuation:

- full evacuation – evacuating everyone at once.
- partial evacuation – evacuating part but not all of a site. For instance, if you have more than one building on your site, you may not need to evacuate all buildings, this would be relevant for Higher Education settings. Keeping people within buildings not directly targeted may provide some protection from flying glass and debris in the case of a bomb threat or mean that you can lockdown that building in the case of armed someone intending to cause harm.
- phased evacuation – evacuating people in order, often with the closest people to the threat evacuated first. This should be considered to reduce crowding of exit routes.
- directional evacuation – advising evacuating people to only use certain exit routes, to avoid sending people closer to the threat.

Your incident response plans should consider how you could put in place these different types of evacuation and communicate specific evacuation instructions to staff, as well as how you would respond if the safety of routes changed during an incident.

Options in an extended evacuation

Once a situation has become more stable and it is likely that your site will remain closed for a substantial time, you can consider whether it is appropriate to enact plans to send learners and staff home if safe to do so. Only allow people to move away from muster points if you can be sure that they will not re-enter any unsafe areas, for instance to attempt to retrieve personal belongings.

After moving people to a place of safety, a designated member of staff should prevent individuals from re-entering an unsafe area. When the police arrive, they will cordon off the danger zone.

The member of staff should also identify who is not present, and coordinate efforts to contact unaccounted individuals.

Naming exits and routes

If you do not already have strong names associated with building areas or exit routes, consider how to refer to buildings, corridors, and stairwells to make navigation more straightforward.

Evacuating to a safe location

Evacuation will need to be to a safe location at a safe distance away from the threat. The safe distance depends on the possible size and type of the suspicious item.

Safe distances

15 meters – do not use your mobile phone or any radios/electronic devices within 15 metres of the suspicious item. 15 meters is about the length of 3-4 cars.

100 meters – move at least 100 meters away from a small item, such as a rucksack. This is the recommended minimum evacuation distance where there may be a risk to life.

200 meters – move at least 200 metres away from a small vehicle or large item, such as a car or a wheelie bin.

400 meters – move at least 400 metres away from a large vehicle, such as a van or lorry. This may be several streets away.

Muster points are planned safe locations where people can gather during an evacuation and wait for the incident to be resolved. You may need different muster point arrangements for different sizes of hazard, and they may be further away than the muster points for fire hazards. Planning in advance a range of possible muster points give staff a range of options during an incident. Clear names for the various muster points will help the Incident Lead advise staff which ones to use during an incident and help staff co-ordinate what is happening at different locations.

Staff need to be aware of the range of identified muster points, but you should avoid making information about muster points publicly accessible, so that someone intending to cause harm cannot use those locations to target evacuating people in secondary attacks. This includes signage about muster points and readily accessible information online or on noticeboards at the site. You are advised to consider including the principles of security minded communications (preventing information being publicly available where possible that could be beneficial and used by a someone intending to cause harm).

Schools should therefore not circulate plans online and should consider using alternative ideas such as colour codes/shapes instead of signage at muster points. This would be most helpful for learners with SEND, to ensure they are at the correct muster point.

To plan your muster points, consider:

- the straight-line distance to the muster point from where the bomb or suspicious item might be located.
- does your setting have hard cover (such as concrete or brick) at these muster points, to provide additional protection from flying debris?
- are there secondary hazards nearby, such as glass from windows and skylights, or parked vehicles?
- are you out of line of site of where the bomb or suspicious items might be left?
- is the risk posed by other hazards at the muster point low and manageable (e.g. road traffic)
- can you clearly communicate instructions about which muster points to use during an incident? Can you name each location so that staff and learners can easily understand where to go during an evacuation?
- how many people could wait safely and comfortably at each muster point?
- if too many people arrive at a particular muster point, how could you safely move people to a different muster point with more space?
- do staff at muster points need a way of communicating with one another?
- how will this work in practice for learners with SEND?
- do you need to coordinate the use of muster points with surrounding settings to ensure they are not being used by others at the same time for their evacuation muster points?

Personal Emergency Evacuation Plans (PEEPs)

Learners and staff with disabilities may not be able to evacuate as quickly or as easily as others in an emergency, or their routes may be more limited.

If there are learners or staff in your setting who require a PEEP for a fire evacuation, you need to also plan their personal emergency response for a range of security incidents.

Educational settings should make adjustments to the generic plan to consider the impact of disability and plan holding areas where necessary; this includes making alternative arrangements for learners with SEND.

The Emergency planning and response for education, childcare, and children's social care settings provides further guidance for SEND and specialist settings.

Communicating during an incident

Planning how you should best co-ordinate a good emergency response to a range of incidents requires you to think through what you will communicate with different people and how you will do this. Having tried and tested communications plans and procedures will give you a framework to apply to the unique and unforeseen incident that you face.

It is important to plan your communication methods in advance and any code word or signals you may need to use. The Incident Lead should consider how best to communicate to staff and learners. They will need to give clear and concise instructions, while avoiding giving someone intending to cause harm information that could be used to put anyone in greater danger.

Managing an incident includes coordination with staff and those directly involved in the incident, the police and other emergency responders. It requires compassionate communication with parents and carers, and you may also need to respond to general interest from the public and media.

Some considerations will be more important in certain types of incidents than in others. For instance, staying silent and hidden may be a priority in a particular lockdown or invacuation response, so that you do not draw attention to your location. In an evacuation response, having portable communications methods becomes more important, and noise is less likely to be important. In an ideal world, you might have a single communications method that is suitable for all scenarios. However, in the real world, your best strategy may be to prepare a number of communication options and make sure that all staff are familiar with their strengths and drawbacks in different incidents.

Communicating about the threat across your setting

The first alert needs to ideally:

- be quick to activate.
- reach the people who need to know, which is normally everyone on the site, both teaching and non-teaching staff, catering and cleaning staff etc. You should consider whether it would be appropriate for the alert method to reach younger learners.
- be something that any member of staff could activate from various locations, or you should have alternative arrangements in place for if you cannot reach your main method of alert.
- not provide any information on the locations of people on the site.
- not increase the risk of harm to the person who activates the alert.

Possible options:

- use of existing alarm systems such as fire alarms
    - the alarm must differ in some way from the actual fire alarm sound, which would automatically lead to evacuation. Could another alarm tone or an intermittent sound be used for a threat?
- use of internal phone systems
    - would this method be quick enough?
- use of a tannoy system, possibly in combination with incident codes
- using a silent broadcast or emergency alert system on staff's devices
- using an instant messaging app on phones or other devices
    - would this get the alert to everyone who needed it, for instance, would this method work for catering and cleaning staff?
    - would everyone see this immediately?
    - how would you keep the group membership up to date?

Developing your own incident codes

A coded message can quickly convey a message to staff without scaring learners who hear or see it and without giving away information to any intruder.

You can devise your own system of incident codes for communicating about an incident across your setting. You could consider:

- mimicking a normal announcement, e.g. "Could Mr XXXX report to reception," where staff know that there is no such person
- using a set of colours, numbers, trees, or anything else
- whether you use the codes to describe the type of incident, or the type of overall site response needed, or both

If using incident codes, it is essential that staff distinguish these critical incidents from any other normal announcement and recall what the codes mean. You must plan how you will induct and train staff in your incident codes.

Methods for ongoing communication during an incident

The Incident Leads and staff in the setting need one or more communication methods to exchange information and instructions with one another during the incident, until the police and emergency responders arrive. Staff may be dispersed within a building or may have evacuated with learners to scattered muster points.

The communications method should ideally:

- be silent and invisible to someone intending to cause harm, so that you do not draw unwanted attention to your location.
- enable two-way communication, both with the Incident Lead and preferably also with other staff members. This would help you inform others about what is happening at your location.
- be portable, not too heavy or bulky to carry, and not dependant on your normal WiFi and wired connections. A portable system would particularly support co-ordination between evacuation muster points away from your site.

Communicating silently with learners in your care

Staff may need to communicate with learners to provide reassurance or to convey a new plan to moving location. However, in a situation where someone intending to cause harm is moving through a building, keeping communications out of sight is essential. Staff need to take into consideration the needs of all learners particularly learners with SEND who may need alternative forms of communication such as utilising written communication skills or physical sign language.

Possible options:

- writing on a whiteboard, a tablet or paper (check whether intruders could notice this through windows or doors)
- physical gestures and body language

Communicating with the police

During an incident, the role of the police emergency response may include:

- leading the incident response once on site.
- advising on the incident response, even before arriving on site.
- working in partnership with your setting's Incident Lead and all staff present
- armed police being deployed to resolve the incident.

Call handlers should give the police as much information as possible. Consider using the ETHANE model (see ANNEX D) for reporting incidents. The police will ask prompt questions to help you explain what you know:

- what has happened? If you are reporting a suspicion, what makes the incident suspicious?

- where? Give as much detail as possible: the address or general location, where in the school grounds the building in question is located and how to access it, so that police can head straight to the right place.
- when? What time did this happen?
- if the incident involves people, do you know their identity, can you describe them, their clothing and any weapons? Where are they going?
- if the incident involves a suspicious object, describe the object and where it is located?
- what actions have you taken?

Further information such as number of casualties, type of injury, hostages, building information, entrances, exits or providing police with a site plan when they arrive on site will help police response.

Seeing armed police arrive can be an unsettling experience, for you and the learners you are with. Staff need to role model the correct behaviour for the learners that you are looking after:

- follow the police officer's instructions.
- remain calm.
- avoid sudden movements that may be considered a threat.
- keep your hands in view.

Initially, officers may not be able to identify the attacker. As such, when they come across you, they may:

- point guns at you / your group.
- treat you firmly.
- question you.
- be unable to distinguish you from the attacker.
- officers will evacuate you when it is safe to do so.

Communicating with parents and carers

The incident may cause unwanted attention from the public and concerned families may want to be at the scene of the incident. However, this could make the situation more dangerous.

The police will have a pre-prepared communications plan including messages, general holding statements and lists of media contacts. They will also decide when to publicly communicate about the incident. Sensitive communication around any casualties is strictly controlled by the emergency services.

The initial communications to parents and carers should come from the setting, rather than the police or through social media. Settings should communicate promptly about the incident taking place to reassure parents and carers that the situation is being effectively managed. When communicating, settings should be clear that parents and carers should temporarily stay away from the site. You should aim to establish your communications channel as the best source of information about the incident, so that parents and carers are less likely to rely on unreliable reporting through their own instant messaging groups and other social media channels.

You should prepare in advance a selection of holding statements suitable for a range of incidents, and ready for issue (with minor amendment) to send to the primary contacts of the learners in your setting during the initial phase of the crisis. For instance:

Example A

“There has been a security incident at [name of setting]. We have taken precautionary measures to evacuate/lockdown the site temporarily to keep learners safe. Our staff are looking after all learners and the police are also on site to resolve the incident. For everyone’s safety, please stay away from the site. We will provide further updates using this method. We will inform you about any arrangements to collect your child/allow your child to go home when the incident is resolved, and normal activities are resumed.”

Example B

“An incident has occurred at [nearby location] and we have been advised by [the local police force] to put in place a lockdown. We would like to reassure you that learners are safe and well. We have a police presence on site and are being fully supported at this time. We ask that families and friends do not come to [name of setting] at this time as this could compromise the police operation currently underway and compromise the safety of the learners. We also ask that you do not attempt to communicate with the University office so that staff can prioritise supporting learners and liaising with the police. We thank you for your support and will update you as soon as possible when we know more.”

You should consider how you will access your pre-prepared holding statements if you were locked down, invacuated or evacuated.

The experience of some settings is that their phone lines have jammed up during an incident with concerned parents trying to find out about their learners. While well worded holding statements can help to mitigate this, it could still be a risk. You should consider whether this would cause problems for you, for instance would you still be able to dial out to the police, and how would you work around this.

Communicating beyond your setting

Alerting others

A security incident in one location could affect homes and businesses nearby. You should consider how you could alert others outside of your setting to the incident so that they can take appropriate action. This should be included in your incident response plans with contact details so that you are able to communicate with them.

Requesting support

Businesses and partners outside of your setting may be able to help and support you during an incident. You should consider in advance who you may be able to call on for extra support from outside your setting, such as your local authority, your local governing body, local businesses or other local partners.

Local Resilience Forums are multi-agency groups, involving the local authority, police, emergency services, organisations and businesses. They encourage local co-operation in planning how settings will respond to incidents. You may proactively wish to find out about their work and who is representing the education sector in your area, for support in your own planning.

Handling the media and social media content

Responding to the media and social media pressures are low priority in comparison to the immediate incident response to bring learners and staff to safety. It is likely that there may be a high level of public interest in the incident, and you may reach a point where you feel a response is required. This will help to control the situation and should help to regain privacy for those affected, however settings are not obliged to communicate with the media if they do not want to.

It is best to communicate through media and social media channels after communications have gone out directly to parents, carers and family members of the staff and learners involved in the incident.

Be guided by police advice on social media use and what should be shared with the public. There is a risk that these uncontrolled communications create panic in the wider community, and harmful misinformation could make the incident worse.

To mitigate this risk, you should consider:

- whether discussing incident preparedness with learners is suitable, if so, include the requirement to not use phones or other devices and to not post about the incident on social media or in messages to friends and family.

- when appropriate, during an incident remind learners and any visitors or members of the public to not send messages or post on social media about the incident.
- what communications are and are not appropriate for people facing considerable waits during an incident, for instance after evacuating to muster points or during an extended invacuation or lockdown.

Related sections and resources in this guidance:

- you should start to set out plans for communicating during an incident using the template protective security and preparedness plan (available in the Interactive resources section)
- you should adapt the template summary of lockdown, invacuation and evacuation options (available in the Interactive resources section) to add your setting's incident codes to this sheet that could be included in grab kits

Compiling your grab kits

Your setting will already have first aid and fire safety equipment available, as required by your health and safety and fire risk assessments. You may need to use this equipment during the incident.

Grab kits may also be helpful to include additional equipment that may be required during a terrorism incident response. A grab kit is a selection of essential items that you may need during an incident. These should be prepared in advance and left in convenient locations. Staff should not put themselves in additional danger to collect a grab kit.

You should minimise the number of different items that staff need to grab in an incident and should consider including any communications equipment, useful information, and Public Access Trauma first aid kits.

Communications equipment

This is equipment that can assist you to communicate with colleagues and/or parents during an incident. Equipment can include electronic devices or utilising written methods of communication where pen and paper is required in which case, you may want to pack a notepad with some pens and paper in your grab kit.

Where key information and communication apps are stored on devices, you should place a device next to the grab kits so that it is easily accessible. These devices should be placed on silent. Where key information is held on paper-based records, settings should consider how staff will be able to bring this with them during an incident, where necessary.

If using electronic devices, you should remember to include any login details, power cables and supplies are included in the grab kit.

Useful Information

You should consider what useful information you should include in the grab kits and ensure that these are kept up to date. Information to include in grab kits should include:

- site plans to assist local police.
- attendance registers and visitor logs.
- contact details: emergency contacts for learners and staff, contacts of businesses nearby who you may need to warn, essential contacts who will be able to assist you during an incident.
- bomb threat checklist (tailored in advance) and a pen/pencil.
- lockdown/invacuation and evacuation template (completed in advance).

- medication lists, reasonable adjustments or tailored plans particularly for those with SEND.

Public Access Trauma first aid kits

A Public Access Trauma first aid kit (PAcT) is a first aid kit which supports the treatment of immediate, life-threatening injuries. The kits are designed to be used by anyone, regardless of their level of first aid training and are usually located in publicly accessible locations for people to easily access.

Settings should consider having PAcT kits readily available. There is no duty to make these available, but you should consider them for your setting. They may need to be kept separate to other grab kits so that they are publicly accessible.

When compiling your grab kits you should also consider:

- what equipment should be included in the grab kits i.e. pens and paper, bottles of water etc.
- what equipment should be included for SEND learners i.e. oxygen machines, medications etc.
- the number of kits your setting needs and whether you need separate kits for specific learners i.e. learners with asthma who need inhalers, learners with anxiety who need safety behaviour equipment
- where these grab kits will be located

This is not intended to be a fully comprehensive list, and you may also add other items that you think could be useful during an incident.

Writing, testing and implementing your protective security and preparedness plans

You should consider whether the protective security and preparedness plans that your setting needs should be written into a new policy or integrated as additional annexes within existing policies and plans. Some settings address protective security and preparedness objectives within critical incident plans, major incident plans or other security policies and plans.

Objectives of protective security and preparedness plans

Settings should have plans in place to reduce the risk of terrorist incidents by making it difficult for a hostile to target their sites. All staff should understand the actions they can take to be part of a good security culture that reduces the risk of an incident.

Settings should have plans in place to respond effectively to different types of incidents. If an incident does arise, staff should be able to draw on their knowledge of your plans and make good judgements about how to keep themselves and others safe.

You should test out your plans to make sure they are suitable and remain effective.

Consulting members of staff, management boards and governing bodies (or their equivalent for your setting) can help raise awareness and ensure plans are robust. If your school is part of a trust, you should also inform the trust.

Writing and improving your plans is an iterative process that should be informed by different types of engagement activities. This should include obtaining feedback to inform and strengthen your plans. Feedback can come from a range of engagement activities, such as discussions with senior colleagues, training and drills for staff to assure the plans and advice from local authorities or local police.

Writing your protective security and preparedness plan

Your protective security and preparedness plans should cover:

- the context and purpose of the policy.
- leadership, accountability and assurance.
- staff roles.
- training staff.
- security culture.
- grab kits.
- communicating during an incident.
- response options: RUN HIDE TELL, lockdown, invacuation, evacuation.

Summary documents you are using in your grab kits (such as a bomb threat checklist and a summary of your lockdown, invacuation and evacuation procedures) would be good to include as annexes to your plans.

Involving others to implement and test the plan

Training your staff will give them a basic knowledge of the topic of counter terrorism and your setting's incident response plans.

Testing and exercising will show you how well your incident response plans and procedures work.

Drills will help people embed their theoretical knowledge and give them experience of how to react during an incident.

Training staff, including inductions

You should seek ways to embed up-to-date protective security awareness and preparedness work within your continuing professional development plans for all staff and in inductions for new starters, so that you maintain a good security culture over time.

Staff training should include:

- general protective security awareness, for example ACT for Youth.
- ACT for Education e-Learning is free training aimed at all staff working in education settings and will teach learners how to identify security vulnerabilities, suspicious activity and how to respond when there is an attack.
- the contents of your incident response plans - how will staff know to lockdown, invacuate and evacuate, and how will they receive specific instructions?
- consideration of SEND learners/staff.

- the individual's role in implementing the plans - what is expected of them if they have to lockdown, invacuate or evacuate? How do they fit into the wider picture?
- what is the role of the incident lead? Who would normally be in this role and what would happen if they are not available? What decisions do the Incident Lead have to make and what do they need to make sure gets done?
- how all staff can be part of a good security culture that deters, detects and mitigates against terrorism, other criminal activity and other forms of anti-social behaviour.
- any additional training that staff may need so that they can use communications equipment, first aid equipment, fire safety equipment or other grab kit equipment during an incident, or any specific training for people with specific incident response roles such as marshals.

Discussions within staff teams, and age-appropriate lessons for learners, can also be part of training for the people in your setting.

Testing plans through exercises

Exercises simulate emergency situations to test procedures. There are three types of exercises: discussion-based, table-top, and live play.

Discussion-based exercises

Discussion-based exercises are cheapest to run and easiest to prepare. They can be used at the policy formulation stage as a 'talk-through' of how to finalise the plan. More often, they are based on a completed plan and are used to develop awareness about the plan through discussion.

Table-top exercises

Table-top exercises usually involve a realistic scenario where players are expected to know the plan and they are invited to test how the plan works as the scenario unfolds.

This type of exercise is particularly useful for validation purposes and for exploring gaps in procedures. Table-top exercises require careful preparation but are relatively cheap to run; the main cost being staff time.

Live play exercises

Live exercises are realistic rehearsals for implementing a plan, using your normal site and facilities, and taking place in real time. Live exercises are particularly useful for testing logistics, communications, and physical capabilities.

They require more time, preparation, and budget than other exercises. This robust method of testing is particularly appropriate for settings on large and complex sites, and settings with dedicated security staff, although they can also be considered for smaller sites.

As a secondary objective, live exercises also make excellent training events. They can help participants develop confidence in their skills and provide experience of what it would be like to use the procedures in a real event.

Major venues and visitor attractions prepare for months to run complex live exercises, involving multi-agency collaborations with large-scale use of actors. While this may not be possible or proportionate for settings, a simplified version should be considered. Leicester De Montfort University ran a live exercise that tested out some of their physical security measures that can be seen in ANNEX C.

How to plan an exercise?

Decide what type of exercise you will run and set the objectives

Settings should consider what they hope to achieve from their exercise and ensure that everyone participating understands these objectives. These should include:

- testing your security infrastructure.
- assuring your incident response mechanism.
- testing readiness of staff and senior team.
- liaising with local partners to ensure effective collaboration.
- scrutinising existing plans to identify weaknesses.
- finding solutions for any identified issues.
- facilitating open and honest conversations.
- achieving senior buy-in on next steps.

Make sure participants are ready for the exercise

To test incident response plans and procedures, participants need to be trained beforehand. Settings should plan how senior leaders will be involved in the exercise or in a position to observe what happens. Staff should be informed of when an exercise will take place and that they will be observed to test the procedures in a controlled environment. It should be made clear to staff that this is a test of procedures and experience rather than a test for staff.

Consider baselining to identify your security vulnerabilities

Baselining is a process to understand the current security measures in place at a setting. It will identify any vulnerabilities and opportunities that someone intending to cause harm may exploit during either the information gathering or attack phases. Understanding your security vulnerabilities can help you identify the types of scenarios that your incident response plans need to address and set the right objectives to test these aspects of your plans. This is particularly worthwhile before conducting a live exercise to make sure that it is well focused. Baselining can also be used to help focus a table-top exercise on useful objectives.

Baselining can include:

- conducting hostile reconnaissance of your site:
    - what information can be found about your site online?
    - how easily can information on your site be accessed?
    - how easily can photos or videos be taken of key infrastructure?
    - how much information can be accessed to make your site an attractive target?
- attempting to gain access at your site
    - how easily can someone without a pass access your site?
    - how easily can someone walk through your site without being challenged?
    - how easily can someone access secure areas?
    - using high-vis or other props to look like a contractor (such as a ladder or trolley) how easily can someone blend into the surroundings without actually having official access?
    - walk the boundary of your site, looking in as if through the eyes of someone wanting to gain access. Where are the weak points and the hiding places out of sight of staff and CCTV, and what should you do to strengthen them?

Baselining may require the assistance of an unfamiliar person. If you have good collaboration with local police, they may be willing to offer advice and assistance to your exercise and planning.

Learning lessons

An important part of the exercise is reviewing and recording what went well and what could be improved. Consider the exercise from start to finish.

- had this been a real attack, what would the impact have been?
- how could this response be improved?
- has an additional training requirement been identified?
- what changes would make this type of incident harder for someone intending to cause harm to carry out?

Plan and implement improvements

There may be various ways to mitigate the risks that you have identified through your exercise. Where a cost applies (such as buying new equipment), the results of your exercise provides evidence of risk and vulnerabilities to help you secure the budget. If costs are a barrier to certain changes, then record this too, and consider how you can mitigate the risks in other ways.

Examples of different possible mitigations to problems identified in an exercise

Problem identified: Intruder not noticed on CCTV.

Possible mitigations:

- make sure existing CCTV is fully working and unobscured
- train security/reception staff on CCTV tracking
- upgrade CCTV equipment
- can you make those areas not covered, harder to access

Problem identified: Lockdown response was inconsistent across the site.

Possible mitigations:

- identify reasons for inconsistency and improve plans accordingly
- improve use of communications systems and processes in a lockdown
- train staff on what they should do in a lockdown
- invest in centralised lockdown system
- retest procedures to understand improvements

Make sure that your protective security and preparedness plans and any other relevant plans or policies are updated to reflect the changes agreed.

Regular testing and exercising

When you have determined how to mitigate the vulnerabilities identified through your testing, staff should be trained on these changes and the plans should be tested again.

A rolling programme of testing and exercising is recommended to ensure your setting remains as prepared as possible.

- you should use or adapt the template protective security and preparedness plan to draft your own policies and plans
- when you have written, tested and implemented your protective security and preparedness plans, you should go back to the quick self-assessment – how prepared is your setting? You can use it to check the progress made since your first self-assessment and highlight the improvements and identify any further gaps.

Post-Incident Welfare

Your plan should consider the emotional and mental impact on learners and staff within the setting as well as parents. It may be helpful to introduce a strategy that will monitor learners and staff who are primarily affected by the incident.

There are many ways in which individuals will have been affected by an incident. Some may have suffered a bereavement; others will have been physically injured or experienced emotional or psychological trauma. It is important that the setting offers learners and staff the opportunity to access psychological support and counselling; ensuring that learners and staff know that support is available, and help will be given to arrange access to these services.

Continued support is essential as victims may need support for months or possibly years after an attack. For example, if a Year 6 learner has been affected by an incident and is transferring from primary to secondary education, you may want to consider notifying the headteacher of the new school to put ongoing support in place.

There are a number of resources available to support settings to support those affected:

- Support for Victims of Terrorism: this support page provides various guidance and links to support organisations including advice on dealing with anniversaries, handling media attention and helplines for both adults and children.
- Guidance on how to support a victim of terrorism: this guidance can be used for family, friends, peers and the community surrounding victims of terrorism to help them to support the person that has been affected by a terrorist attack.
- Leaflet on the support services available: this leaflet summarises the support services available for victims of terrorism which can be shared with teachers, families, friends and peers. The leaflet explains how to access support services available.
- Help and support after a traumatic event: the NHS guidance on further resources and support.
- Emergency planning and response for education, childcare, and children's social care settings guidance: this guidance helps education, childcare, and children's social care settings plan for, and respond to emergencies with particular guidance on wellbeing and support as well as other areas to consider such as exam and assessment disruption.
- Victim Support operates a 24/7 support line, offering emotional and practical support to victims of terrorism. The number is 0808 168 9111 and is free to call.
- Samaritans offer emotional support and a safe place to talk at any time. The number is 116 123 and is free to call.
- NHS Choices outlines mental health symptoms and how to seek help.
- NHS: Coping with stress following a major incident

- NSPCC: How to have difficult conversations
- Red Cross: Talking with children about a major emergency (5–11 year olds).
- Red Cross: Talking with young people about a major emergency (11-19 year olds).
- UK Safer Internet Centre and NSPCC have guidance and resources to help keep young people safe online.
- Searching, screening and confiscation.
- UK Trauma Council have resources to help educators identify, help and support traumatically bereaved children and young people.

Post-Incident Reviews

Post incident evaluation is essential for all those affected within the setting and business continuity plans are an integral part of security policy that should be embedded.

The setting should consider having a full debrief obtaining feedback from all key people involved. This will enable the setting to understand what measures need to be taken to support victims and also, allows the setting to incorporate a 'lessons learnt' plan to improve internal security policies and procedures within the setting.

In slower time, the setting should debrief with neighbouring settings and businesses, local authorities and police.

The School and College Security guidance helps settings to manage their security effectively and provides relevant information and resources to support settings during recovery. The guidance also has a number of templates and checklists that could be used including the Post Incident Support Checklist.

Annex A: Links to resources

Education settings should use the resources available within this guidance and seek further advice from their local authority education leads (who hold a relationship within the local authority and/or Local Resilience Forum regarding planning procedures for these types of incidents).

Settings should also contact their local policing contacts (who lead on the initial response to any incident). This will enable them to discuss their plans, coordinate any local police response procedures and ascertain whether any other support might be available.

Related content on ProtectUK

Posters are both useful reminders of key security principles for all staff, and also promote a good security culture in your organisation that will deter someone intending to cause harm from seeing you as an easy target.

- HOT protocol poster
- Suspicious items poster
- Good housekeeping | ProtectUK
- RUN HIDE TELL poster
- RUN HIDE TELL video
- Bomb Threats Action Card poster
- Standards for Public Access Trauma (PAcT) First aid kits – equipment | ProtectUK
- Supporting information for public access trauma first aid kits | ProtectUK
- Act for Youth
- ACT for Education e-learning

Useful external links

- SCaN for All Staff | NPSA - this all staff training module is designed for all members of staff across an organisation, venue or event, to increase their awareness of hostile reconnaissance and how they can help counter it. The principles of See, Check and Notify can easily be translated into an education environment. SCaN for all staff training is free. It can be accessed in different ways:
    - individual learners can access a 15-minute video and quiz.
    - groups of learners can access facilitation materials as well as the video to run a 30 minute or 60 minute (recommended) interactive session. This can be led by any member of staff.
    - the training can be embedded into your setting's own e-learning system.

- Disrupting someone intending to cause harm reconnaissance – provides general guidance from NPSA
- Protecting your assets – provides guidance on NPSA's protective security methodology, appropriate to more complex sites such as larger schools, further education colleges and universities.
- Action Counter Terrorism (ACT) website where you can report suspicious activity online and in confidence.
- Marauding Terrorist Attacks – provides detailed guidance from NPSA, including a short animation and short film about lockdowns.
- Protected spaces – further guidance from NPSA about invacuation to protected spaces.
- The Catalogue of Security Equipment | NPSA – helps identify appropriate physical security equipment that has been evaluated against specific NPSA security standards and achieved the requisite performance rating. If you are considering buying security equipment, first contact a Counter Terrorism Security Advisor (CTSA) via your local police force and ask for their advice and support.
- handling media attention after a major incident – more detailed guidance on gov.uk
- how to make a silent 999 call – provides information about using 999 while remaining silent.
- First aid in schools, early years and further education - GOV.UK (www.gov.uk) – non-statutory guidance for employers in early years, schools and colleges.
- Emergency planning and preparedness: exercises and training – provides guidance on training and exercising from the Cabinet Office.
- Exercise Planners Guide - provides guidance to those who have to design and carry out emergency exercises.
- Counter Terrorism Security Advisors (CTSAs) in police forces: You may be located somewhere where Policing Counter Terrorism Security Advisors (CTSAs) operate but it is important to note that CTSAs only work on a 1-2-1 basis with individual sites that have been deemed at higher risk or other individual settings where a real and credible threat has been identified and confirmed. They are a finite resource and only provide bespoke advice to those individual settings to support the reduction of site-specific security vulnerabilities.

Additional guidance

All schools will have policies, plans, and procedures in place to deal effectively with health and safety responsibilities. Guidance, training and advice on safety and security can be found:

- School and college security is non-statutory guidance to help schools and colleges develop policies and plans to manage and respond to security related incidents.

- Emergency planning and response for education, childcare, and children's social care settings is non-statutory guidance to help settings plan for, and respond to a range of emergencies.
- Security Minded Communication helps protect an organisation by viewing existing and planned communication through the eyes of someone intending to cause harm.
- National Protective Security Authority (NPSA) are the UK Government's national technical authority for physical and personnel protective security.

Annex B: Examples

Example showing the stages of creating and refining new protective security and preparedness plans, and how different activities can strengthen those plans.

Writing a plan and knowing when to involve others

1. Draft your protective security and preparedness plan.
2. Involve others by holding a discussion-based exercise for senior management to test the content of the plan.
3. Use this information to finalise and agree your plan.
4. Involve others by training staff on your plan.
5. Hold a table-top exercise involving more staff to test out your final plan and identify any final improvements to be made.
6. Review and refine your protective security plan.
7. Involve others by conducting drills to embed knowledge and develop experience.

Table-top exercise example

A table-top exercise will work to validate your plans, give staff practice in carrying out roles and test procedures.

This example scenario aims to test your setting's response to an armed incident taking place at your premises. There are three inputs which together tell the story of how the incident unfolds. After each input, there are prompt questions to help your team discuss how they would react to that situation.

You could adapt this example to work through your responses to different types of incidents, such as someone intending to cause harm on the premises or a suspected bomb on or near the premises. You could also adapt the example to make sure that elements of your incident response are tested. For instance, would your response change if the incident occurred when people were outside rather than inside the buildings?

This table-top exercise is designed to last approximately 2 hours.

Plan

Timings	Activity
10 minutes	Introductions and recap of objectives
5 minutes	First input
20 minutes	Group discussion
5 minutes	Second input
20 minutes	Group discussion
5 minutes	Third input
20 minutes	Group discussion
30 minutes	Evaluation and next steps

First input

Scenario context: It is Tuesday at 10 am. All staff and learners are in their morning lessons.

Phone Call: A neighbouring school (200 metres down the road) calls the office. They tell you there is an incident taking place outside their premises. They are not sure of the details, but they heard shouting and screaming. One person has suggested that at least one person has a weapon. They tell you the police have been called but there is concern the incident may be moving up the road towards your premises.

Information: There is no further information at this point.

Points to consider:

- What would the person receiving the initial call do?
- Consider your incident response plans – how would you implement them in this situation?
- What are the key things to think through at this stage?

Second input

Scenario context: You are made aware of posts on the local social media pages:

- **Post 1** “There is someone running around the street with a knife, trying to attack people. There may be more than one attacker”.
- **Post 2** “What – my kids are at school there!!! What is going on? Does the school know? I am going down there!!”

Information: You can hear shouting outside the school which is getting louder. You hear a scream.

Point to consider:

- Talk through what you would do next.
- Consider how you would communicate with staff across your setting?
- Would you do anything at this stage to inform parents of the issue?
- What will be your key objectives at this stage?

Third input

Scenario context: Tuesday 10.18 am. Further posts on social media.

- **Post 1** “There are people on the ground, I think they are hurt – possibly dead.
- **Post 2** A video is posted showing a man running around directly outside your school with a knife. There are people running in the street, there is a lot of screaming.

Information: You are informed that armed police are at the scene. Some of the armed police may be visible from the school.

Points to consider:

- What would you need to think through here?
- What steps would you take knowing armed police were at the scene?
- Consider other outcomes – what if police were not at the scene yet? Would you do anything differently? Talk through the possible actions you might consider.

Evaluation and next steps

What did you learn from this exercise?

Consider some of the following and record your conclusions:

- how did your plans play out in this exercise?
- were there any gaps in your plans that you had not considered before?
- what were the elements that worked well?
- what elements did not work so well?

- how might these gaps be improved?
- consider partnership working with police and neighbours – did this work well?

Next steps:

- how will this learning be fed into your protective security and preparedness plans, including incident response plans?
- have you identified any training requirements from this exercise?
- would the use of drills (for staff or children/learners) help embed learning?
- are there any new policies or procedures you might need to consider based on your learning?

Annex C Case study: Leicester De Montfort University's live exercise

Leicester De Montfort University ran a simple live exercise to test out some of their physical security measures.

Baselining phase, in partnership with Leicestershire Police

The baselining phase aimed to see what someone intending to cause harm could access before being identified and challenged. The whole university site was in scope for this baselining. The security team and other staff on campus were not warned of the exercise.

The brief for two plain clothed police officers was to:

- access as many "restricted" areas as possible.
- tailgate through controlled access points.
- identify unlocked ICT equipment and photograph.
- access buildings via unlocked/open fire doors.
- remain in buildings after lock ups.
- use facilities freely.
- access student areas .

The police officers disguised themselves with plain yellow jackets and a ladder and used a pretext of searching for a fictitious water leak on a very wet stormy evening in November. The police officers conducted this baselining between 2.30pm and 9.45pm.

After the baselining, the police officers shared their observations with Leicester De Montfort University staff. CCTV footage was examined to help staff understand their security vulnerabilities. The evaluation of this baselining informed the objectives and plans for the live exercise.

Planning and conducting the live exercise

The live exercise tested the response to a simulated incident from security and management. Leicester De Montfort University wanted to investigate specific questions:

- does lockdown work?
- are communications messages ready and deployable?
- are trauma kits available in the case of mass casualties?
- are staff sufficiently trained?
- can we save as many people from harm as possible?
- do we meet the emergency services response requirements?

- do Major Incident Plans work?
- what buildings/areas are accessible to someone intending to cause harm?

Security leads at Leicester De Montfort University planned a scenario simulating a vehicle as weapon attack followed by a marauding knife attack. The live exercise focused on the minutes from the start of an attack until the arrival of the police. The people playing the role of “someone intending to cause harm” wore high-vis jackets so they would be easily identifiable to the security control room.

Some aspects of the scenario were adapted so that other people on site would not be disturbed by the live exercise. When testing hostile vehicle mitigation, the car drove at normal speed but still tested the effectiveness of security bollards by mounting the kerb to avoid them. The person intending to cause harm left the car, and then started walking around the site to approach as many people as possible but did not visibly act out an attack. Instead, they used a tally counter (or “clicker”) to count the number of people they came in touching distance of. Security leads knew that the number of people the person intending to cause harm could approach in the live exercise would be higher than in a real attack, where people would run away. They decided in advance that realistic casualty numbers would be modelled at 10% of the tally count from the exercise.

In the control room, the Head of Security announced the exercise:

> “This is a test exercise; this is a test exercise – A unknown person has driven a vehicle onto campus and has struck several learners. The vehicle is now stationary outside of the “Campus Centre”. The person intending to cause harm has exited the vehicle and has made their way into the “Campus Centre”, believed to be armed. Several casualties are wounded so far.”

Body cameras were activated to record how staff responded.

A second “person intending to cause harm” then arrived at the site and both people intending to cause harm move through the building together, continuing to record how many people they were able to approach. The Head of Security gave a further update to control room staff:

> “Reports are coming in of a second person intending to cause harm on site, entering the VJP building.”

The security control room responded as if it was a real attack. The response was closely monitored by observers watching camera footage from remote locations.

In this exercise, the police arrived on the scene in 12 minutes. The exercise was concluded when a member of the armed response team made physical contact with one of the people intending to cause harm.

Resources required:

- 2 volunteers
- 1 vehicle
- 2 tally counters (clickers)
- 2 high visibility vests
- security team
- CCTV/Control room operator
- private radio channel

Pre-event management:

- NaCTSO informed and in attendance – watching from a remote location
- police in attendance, acting as call handler – watching from a remote location
- senior estates executive – watching from a remote location
- NHS/Fire aware
- no security staff were aware of the exercise before it started

Tips for a successful live exercise

Once the exercise starts, announce to staff that an exercise is underway and they will be observed instead of simulating an attack, which might alarm those unaware of the exercise, use a walk through with an agreed system for counting those coming into contact with the “person intending to cause harm” use high-vis jackets for those involved so they are easily identifiable ensure that senior leaders are able to observe the exercise

Learning lessons from the live exercise

After the live exercise, the security team held a de-briefing meeting with the senior management team and the university leadership to discuss the vulnerabilities identified and the learning from the live exercise.

Glossary

ACT – Action Counters Terrorism.

Bomb threat - is where an individual places an article or communicates information with the intention of inducing a person to believe that something is likely to explode or ignite causing harm within an educational setting.

Counter terrorism (CT) – activities that lower the threat or impact of terrorist incidents.

Education setting – for the purpose of this guidance, educational settings cover settings from Early Years, all schools, Higher and Further Education (including colleges, Sixth Form Colleges and Independent Training Providers), and alternative provisions (including special schools and children's social care settings).

ETHANE – a model for reporting incidents used by the emergency services under the Joint Interoperability Principles in Major Incidents.

Evacuation - moving people outside the building to protect them from a threat in the building.

Grab kit(s) – a grab kit or grab bag is the selection of items that you may need in an incident, which you have previously compiled and left in convenient locations.

Hostile reconnaissance – a critical aspect of detecting and deterring hostile reconnaissance at a site is knowing the threat that you face and understanding where hostiles might conduct their reconnaissance from.

HOT protocol - (Hidden, Obvious, Typical) is the process by which a person decides how to deal with unattended item(s).

Incident – a security issue that affects your setting.

Incident lead – the member of staff responsible for leading the response to the incident.

Incident response – incorporates the overall site response chosen to a given incident, as well as the communications during an incident that are required.

Incident response plan – a plan or range of options that set out how your setting wants staff to respond during an incident.

Invacuation - moving people inside a building to a place of relative safety.

Learners – a person who is learning a subject or skill.

Lockdown - locking or barricading a room's doors and windows to delay or deter someone intending to cause harm from getting into an area.

Marshal – someone with additional responsibilities to supervise and support an incident response, for instance controlling where people are going.

Muster points - planned safe locations where people can gather during an evacuation and wait for the incident to be resolved

NaCTSO – National Counter Terrorism Security Office.

NPSA – National Protective Security Authority.

Overall site response options – referring to the decision to lockdown, invacuate or evacuate, and decision on specific details of the chosen option.

PEEP – Personal Emergency Evacuation Plan

Protect – One of four workstreams of the CONTEST counter-terrorism strategy: Pursue, Prevent, Protect, Prepare. The Protect workstream is about strengthening protection against a terrorist attack.

ProtectUK - a central hub for counter terrorism and security advice, providing everyone with the knowledge and confidence to help tackle threats of terrorism.

Protected spaces - locations within your building(s) that have previously been identified as places of relative safety, where people can hide or shelter from threats.

Protective security – measures that help protect a setting from threats.

Protective security and preparedness plans - the policies and plans that describe how your setting promotes a good security culture that deters someone intending to cause harm from targeting your setting, and how staff should respond effectively to different types of incidents. Settings may use other terms, such as critical incident plans, major incident plans, counter terrorism preparedness plans, or security policies and plans, to achieve these objectives.

RUN HIDE TELL – advice to take in the event of an attack.

SCaN – See Check and Notify.

Security lead – the person responsible for coordinating and overseeing your setting's protective security and preparedness work.

Security culture - a shared set of values which determine how people are expected to think about and approach security in an organisation.

Security-minded communications / comms – the process of considering what of your publicly communicated information might unintentionally assist someone to plan an attack on your setting and taking action to minimise this risk.

SEND - Special Educational Needs and Disabilities.

Someone intending to cause harm - a person who is planning a terrorist incident, another type of criminal activity or anti-social behaviour. (The National Protective Security Authority (NPSA) defines a someone intending to cause harm as ‘a person who wants to attack or disrupt an organisation for profit or to make a political or ideological point’).

Suspicious activity - actions that may indicate pre-operational planning associated with dishonest activity resulting in terrorism or crime.

The ‘power of hello’ - approaching a person behaving unusually to check if things are okay, and in doing so deterring potential criminal activity.

Department for Education

About this publication:

enquiries www.gov.uk/contact-dfe
download www.gov.uk/government/publications

Follow us on Twitter: @educationgovuk
Connect with us on Facebook: facebook.com/educationgovuk