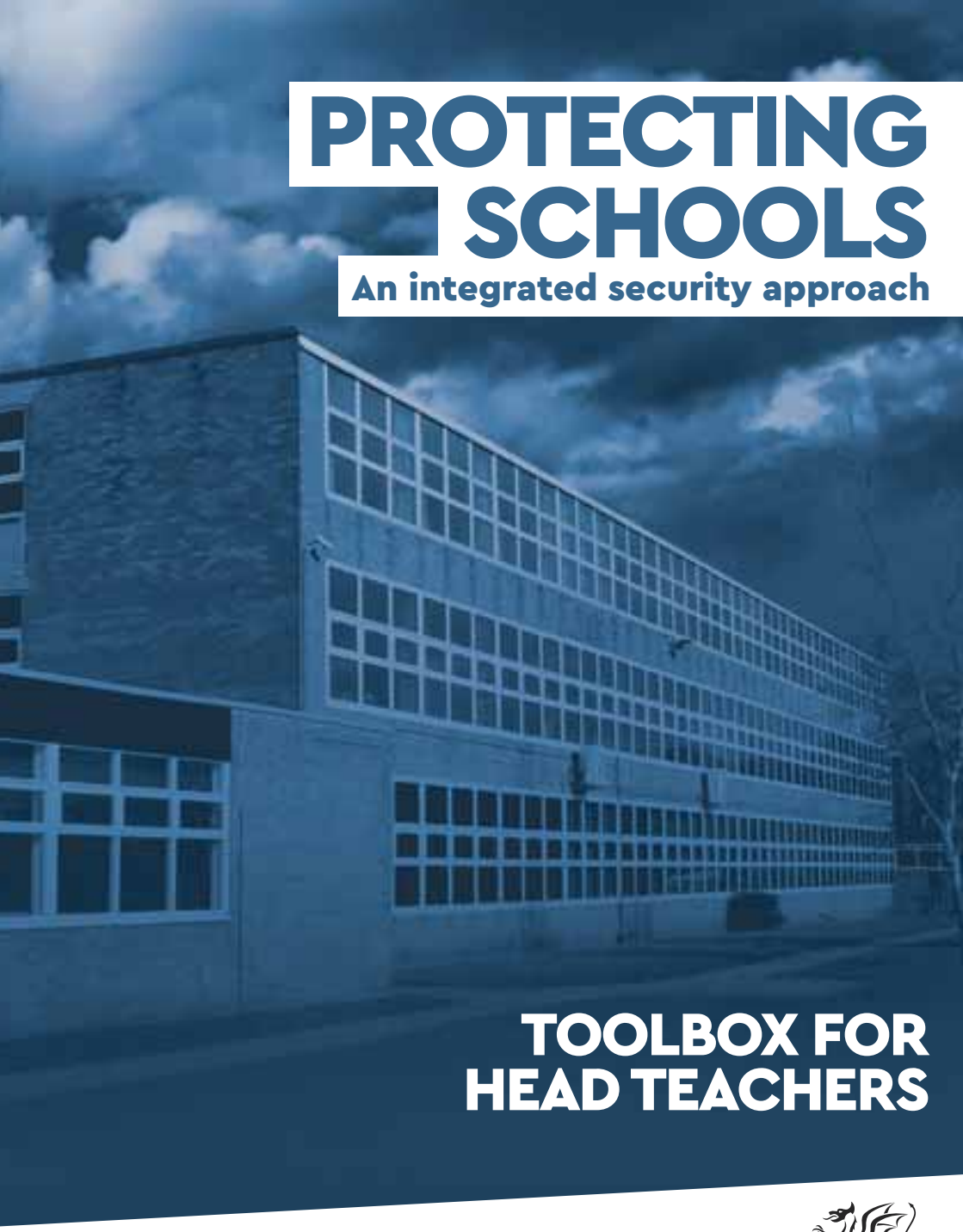


PROTECTING SCHOOLS

An integrated security approach

TOOLBOX FOR HEAD TEACHERS

WECT

Llywodraeth Cymru
Welsh Government


WECTU

CONTENTS

Kirsty Williams AC/AM
Ysgrifennydd y Cabinet dros Addysg
Cabinet Secretary for Education

Llywodraeth Cymru
Welsh Government

To all Cabinet Leads for Education

26th July 2017

Dear Colleagues,

COUNTER-TERRORISM IN SCHOOLS

A key feature of the Counter-Terrorism and Security Act 2015 Counter-Terrorism and Security Act 2015, puts a responsibility on schools to 'have due regard, in the exercise of their functions, to prevent people from being drawn into terrorism and challenge extremist ideas that support or are shared by terrorist groups'. The UK Government published the Prevent Duty Guidance for England and Wales for specified bodies including education providers **https://www.gov.uk/government/uploads/system/uploads/ attachment_data/file/97976/preven t-strategy-review.pdf**

As part of Prevent there is a duty on schools to ensure that staff have the knowledge and confidence to identify those at risk of radicalisation and they are able to challenge extremist ideas used to legitimise terrorism.

To support the implementation of Prevent the Welsh Government has:

- Published and updated version of our guidance document 'Respect and Resilience – developing community cohesion' http://gov.wales/docs/dcells/publications/110209respecten.pdf and this includes an associated self-assessment toolkit. The guidance ensures that schools in Wales have information to help them meet the legal requirements of the Counter-Terrorism and Security Act 2015.
- Developed the Keeping Learners Safe Guidance, http://learning.gov.wales/docs/learningwales/publications/150114-keeping-learners- safe-en.pdf the Welsh Government guidance on the role of local authorities, governing bodies and proprietors of independent schools under the Education Act 2002.
- Developed the HWB website – digital learning for Wales, to include an e-safety zone which contains resources, links, advice and support for children young people, parents/carers and educational professionals and promotes safe responsible use of the internet by all.
- Included a challenging extremism module through Global Citizenship Challenge in the Welsh Baccalaureate.
- Been working with colleagues from the South West Grid for Learning to develop bilingual resources for teachers to provide lessons around online safety.

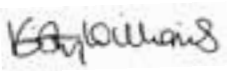
Although issues of national security and counter-terrorism remain the responsibility of the UK Government, the Welsh Government works closely with the Police, Local Authorities and other partners to safeguard people from being drawn into terrorist-related activity.

Following the attacks in London and Manchester I have recently met with the Counter Terrorism Security Advisors from the Wales Extremism and Counter Terrorism Unit WECTU to discuss extremism in our schools. Although at this point in time, there is no intelligence to suggest schools are at greater risk, and it is important to stress that, I feel that there is a need for schools to review their policies and procedures to ensure these are sufficiently robust to deal with such an incident.

I am therefore writing to you to seek your assurance that your schools are supported and have appropriate policies and procedures in place to deal with any form of terrorist attack including lock down in schools.

It is of course important that schools are given specific advice and support on what additional provisions are considered necessary and the support and advice to implement them, if necessary. My officials will therefore, work with you, the regional consortium and WECTU over the coming months to further enhance awareness and training for all education practitioners.

Yours sincerely



Kirsty Williams AC/AM
Ysgrifennydd y Cabinet dros Addysg
Cabinet Secretary for Education

FOREWORD

This guidance has been developed to assist the education sector across Wales in addressing the security issues relating to hostile action. It is the product of discussions and sharing of best practice involving a number of specialist partners including Wales Extremism and Counter Terrorism Unit, Welsh Government and the four Welsh police forces.

Our educational establishments should be places where all students and staff are safe and secure and able to foster a culture of shared values and open debate to cohere the rightly celebrated diversity of the sector. But there is a real and serious threat of domestic and terrorist attacks in the UK and terrorism can come in many forms, not just a physical attack on life and limb. It can include interference with vital information or communication systems, causing disruption and economic damage.

Kirsty Williams AM/AC the Cabinet Secretary for Education said: *'Following the attacks in London and Manchester I have recently met with Counter Terrorism Security Advisors from the Wales Extremism and Counter Terrorism Unit to discuss extremism in our schools. Although at this point in time, there is no intelligence to suggest schools are at a greater risk, and it is important to stress that, I feel that there is a need for schools to review their policies and procedures to ensure these are sufficiently robust to deal with such an incident'.*

The law requires institutions to carry out adequate risk assessments and ensure that suitable measures are in place to manage identified risks. Institutions should conduct prompt and regular reviews of those assessments and measures in light of new threats and developments at the institution and the surrounding area.

Equally important is that business continuity plans address security issues to ensure that institutions can cope with an incident or attack and return to 'business as usual' as soon as possible.

Having a robust security culture and being better prepared reassures your whole community that you are taking security issues seriously.

Heads of institutions should bring this guidance to the attention of all relevant staff. These are likely to include Security, Estates, Facilities, Health & Safety and HR Managers.

Although each institution and venue will have its own particular circumstances, the guidance addresses all of the areas of concern for educational establishments and includes a number of useful good practice checklists.

INTRODUCTION

This guide is intended to give protective security advice to those who are responsible for the security of education institutions, irrespective of size and location. It highlights the part institutions can play in the UK counter terrorism strategy, and how by mitigating the risk you can allow teaching, learning, research, knowledge transfer, community engagement and enterprise to continue as normal.

Terrorist attacks in the UK are a real and serious danger. The terrorist incidents in Manchester and London and the arrests in Wales early in 2017 indicate that terrorists continue to target crowded places; largely because they are usually locations with limited protective security measures and therefore afford the potential for mass fatalities and casualties. The circumstances of the attacks and arrests identify that terrorists are prepared to attack sites well away from London.

Terrorism can come in many forms, not just a physical attack on life and limb. It can include interference with vital information or communication systems, causing disruption and economic damage. Some attacks are easier to carry out if the terrorist is assisted by an 'insider' or by someone with specialist knowledge or access. Terrorism also includes threats or hoaxes designed to frighten and intimidate.

It is possible that institutions could be the target of a terrorist incident. This might include having to deal with a bomb threat or with suspect items left in or around the venue.

In the worst case scenario staff and students could be killed or injured, and the premises destroyed or damaged in a 'no warning', multiple and coordinated terrorist attack.

Of course there is a need to make education institutions as accessible as possible and to ensure there is a welcoming environment. This guide is accordingly not intended to create a 'fortress mentality'. There is however a balance to be achieved where those accountable for security are assured that there are robust protective security measures available to mitigate against the threat of terrorism.

RISK

Managing the risk of terrorism is only one part of an institutions responsibility when preparing plans in response to any incident which might prejudice personal safety or disrupt normal business.

With regards to protective security, the best way to manage the risks to your establishment is to start by understanding and identifying the threats to it, and its vulnerability to those threats.

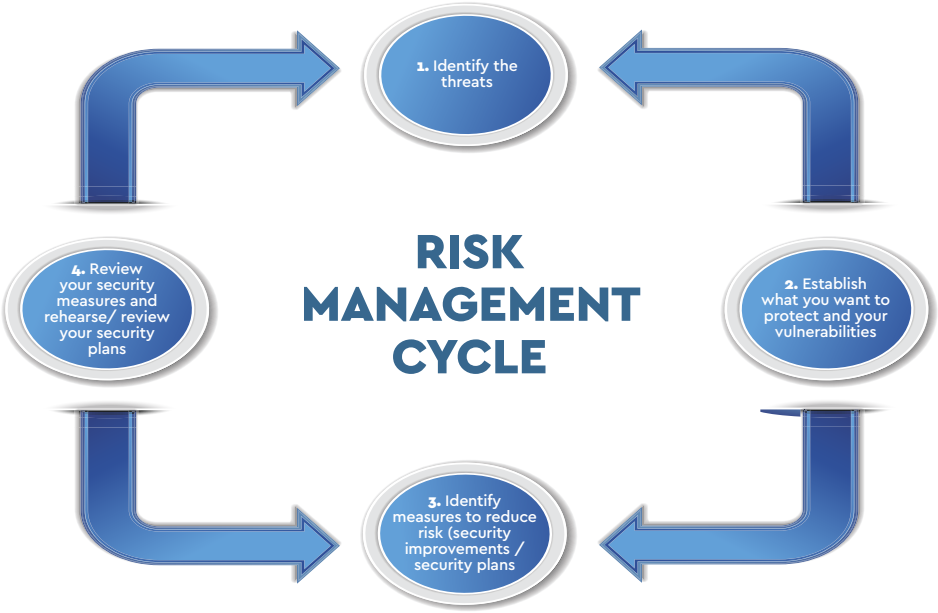
This will help you to decide:

- What security improvements you need to make
- What type of plans you need to develop

For some aspects of institutional security, simple good practice – coupled with vigilance and well exercised plans may be all that is needed.

If, however, you identify areas of vulnerability, you should apply appropriate protective security measures to reduce the risk to as low as reasonably practicable.

The following diagram illustrates a typical risk management cycle:



For further information on RISK please see **www.cpni.gov.uk**

- Adopt a Risk management Approach
- Mitigate your Risks
- Insider Risk Assessment

SECURITY PLANNING

When creating your security plan, consider the following:

- Details of all the protective security measures to be implemented, covering physical, information and personnel security
- Instructions on briefing content to security staff or members of staff with security responsibility including type of behaviour to look for and methods of reporting
- Instructions on how to respond to a threat (e.g. telephone bomb threat)
- Instructions on how to respond to the discovery of a suspicious item or event
- A search plan
- Evacuation / invacuation plans and details on securing the establishment in the event of a full evacuation
- Your business continuity plan
- A communications and media strategy which includes handling enquires from concerned family and friends

Your planning should incorporate the seven key instructions applicable to most incidents:

1. Do not touch suspicious items
2. Move everyone away to a safe location
3. Prevent others from approaching
4. Communicate safely to staff, students, visitors and the public
5. Use hand-held radios or mobile phones away from the immediate vicinity of a suspect item, remaining out of line of sight and behind cover
6. Notify the police
7. Ensure that whoever found the item or witnessed the incident remains on hand to brief the police

Effective security plans are simple, clear and flexible, but must be compatible with any existing plans e.g. evacuation plans and fire safety strategies. Everyone must be clear about what they need to do in a particular incident. Once made, your plans must be followed.

For further information on SECURITY PLANNING please see **www.cpni.gov.uk**

- Security Planning
- Integrated Security
- Cyber Security
- Personnel and People Security

PHYSICAL SECURITY

Physical security is important in protecting against a range of threats and addressing vulnerability.

Put in place security measures to remove or reduce your vulnerabilities to as low as reasonably practicable bearing in mind the need to consider safety as a priority at all times. Security measures must not compromise public safety.

Your risk assessment will determine which measures you should adopt, but they range from basic good housekeeping (keeping communal areas clean and tidy) through CCTV, perimeter fencing, intruder alarms, computer security and lighting, to specialist solutions such as perimeter detection systems equipment.

Specialist solutions, in particular, should be based on a thorough assessment – not least because you might otherwise invest in equipment which is ineffective, unnecessary and expensive.

Successful security measures require:

- The support of senior management including the Director of Estates
- Staff awareness of the measures and their responsibility in making them work
- A senior, identified person within your organisation having responsibility for security.

Remember, you will need to ensure that all necessary regulations are met, such as Local Authority permissions, health and safety and fire prevention requirements.

Plan carefully - as this can help keep costs down. Whilst it is important not to delay the introduction of necessary equipment or procedures, costs may be reduced if the premises or location you are using already has the necessary security which can be easily integrated within your own plan.

For further information on PHYSICAL SECURITY please see **www.cpni.gov.uk**

- Physical Security
- Physical Defences at the Perimeter
- Robust Visitor Entry Processes
- Active Access Delay Systems
- Security Lighting

STAFF SECURITY AWARENESS AND SECURITY CULTURE

The vigilance of all staff and contractors to your venue is essential to your protective measures. They will know their own work areas very well and should be encouraged to be alert to unusual behaviour or items out of place.

They must have the confidence to report any suspicions, knowing that reports – including false alarms – will be taken seriously and regarded as a contribution to the safe running of the establishment.

Training is therefore particularly important. Staff should be briefed to look out for packages, bags or other items in odd places, carefully placed (rather than dropped) items in rubbish bins and unusual interest shown by strangers in less accessible places. Training in emergency response plans should also be included in staff inductions.

What type of security culture do you have, and does this support the demonstration of the right security behaviors?

Security culture is defined by CPNI as 'the set of values, shared by everyone in an organisation, that determine how people are expected to think about and approach security'.

Without the right security values (i.e. culture), employees may pay lip service to the security practices in place, resulting in poor behaviors and lack of compliance with protective security measures. This in turn can lead to increased risk of security incidents and breaches, reputational and financial damage, the development of a climate that facilitates insider threat, as well as potential harm to employees, customers, and/or business performance.

CPNI has developed a tool (SeCuRE) to assist organisations with examining their existing security culture and identifying where and how it may need to change. It can also assess whether the right mix of behavior mechanisms are in place to drive good security practice.

A good security culture in your organisation is an essential component of a protective security regime and helps to mitigate against insider threats and external people threats (such as hostile reconnaissance).

Security culture is the set of values, shared by everyone in an organisation, which determine how people are expected to think about and approach security, and is essential to an effective personnel and people security regime.

The benefits of an effective security culture include:

- employees are engaged with, and take responsibility for, security issues
- levels of compliance with protective security measures increase
- the risk of security incidents and breaches is reduced by encouraging employees to think and act in more security conscious ways
- employees are more likely to report behaviors/activities of concern

For further information on STAFF SECURITY AWARENESS AND SECURITY CULTURE please see **www.cpni.gov.uk**

- Developing a Security Culture
- Security Culture and Behaviour Change
- Create a Strong Security Culture – Soft Measures
- Create a Strong Security Culture – Hard Measures
- Leadership in Security
- Optimising People in Security

GOOD HOUSEKEEPING

Good housekeeping improves the ambience of your site and reduces the opportunity for placing suspicious items or bags and helps to deal with false alarms and hoaxes.

You can reduce the number of places where devices may be left by considering the following points:

- Avoid the use of litter bins next to or near glazing, support structures, most sensitive or critical areas (but if you do, ensure that there is additional and prompt cleaning in these areas).
- Alternatively review the management of all your litter bins and consider the size of their openings, their blast mitigation capabilities and location.
- The use of clear bags for waste disposal is a further alternative as it provides an easier opportunity for staff to conduct an initial examination for suspicious items.
- Review the use and security of compactors, wheelie bins and metal bins to store rubbish within service areas, goods entrances and near areas where crowds congregate.
- Keep public and communal areas – exits, entrances, queues, lavatories – clean and tidy, as well as service corridors and areas.
- Keep the fixtures and fittings in such areas to a minimum – ensuring that there is little opportunity to hide devices.
- Temporary information stands, concessionaires and kiosks should be searched before and after use and secured or moved when unattended.
- Staff rooms and corridors should be kept tidy, and staff rooms should have access control.
- Lock unoccupied offices, rooms and store cupboards.
- Ensure that everything has a place and that things are returned to that place.
- Place tamper proof plastic seals on maintenance hatches.
- Keep external areas as clean and tidy as possible.
- All sites should have in place an agreed procedure for the management of contractors, their vehicles and waste collection services. The vehicle registration mark (VRM) of each vehicle and its occupants, should be known to the security or management in advance.
- If allowed, pruning vegetation and trees, especially near entrances, will assist in surveillance and prevent concealment of any packages.

ACCESS CONTROL

There should be clear demarcation between public and private areas, with appropriate access control measures into and out of the private areas. This relates to private areas within the institution, not public entrances.

Your access control system should support other security measures. Consider system compatibility between access control, alarms, CCTV and text alert systems

Whether driving a lorry or carrying explosives, a terrorist needs physical access in order to reach the intended target.

Access control systems are often the first point of challenge; they represent the boundaries between private and public areas. The level of security in your access control system needs to be a balance between business needs and effective security.

Your personnel security policies and procedures should limit the risk of staff or contractors exploiting their legitimate access to assets or premises for unauthorised purposes. When considering access control security measures security managers need to think beyond an organisation's premises – think also about who else has access to your organisation's information/ databases or other valuable assets, and the locations involved.

Questions to ask:

- Does your school have clearly defined access control guidelines or policies? If so who owns them?
- Where are the access points in your venue (staff, visitors and vehicles)? How are they monitored and protected? How does access control differ for different visitors: staff (are they pass holders), visitors (is security clearance needed), people making deliveries?
- Is the level of protection proportionate to your identified threats (insider threat, terrorism, crime)?
- Are there areas requiring greater or fewer security requirements (secure and non-secures areas)?
- How are security passes and clearances processed – and what checks are required?

For further information on ACCESS CONTROL please see **www.cpni.gov.uk**

- Access Control and Locks

CCTV GUIDANCE

CCTV is often one of the main stays of a modern security system. Its primary focus is to act as a detection and verification system for other security measures. CCTV can be a single or combination of systems and technologies to form the overall security solution, some of these may include:

- Visible band or infrared CCTV
- Thermal Imaging
- Video Analytics

While CCTV, thermal imagers or video analytics are useful technology, all these will rely to some extent on the effectiveness of the control room and the security officer within. The important point here is the ability to quickly monitor an event.

CCTV is normally used to achieve one or more of the following:

- Detect an intruder within a reasonable time frame
- Verify an alarm from a Perimeter Intruder Detection System (PIDS)
- Provide support to a guard or security force
- Provide evidence suitable for use in court

CCTV can help clarify whether a security alert is real and is often vital in any post incident investigation.

If you have access to a CCTV system you should constantly monitor the images captured or regularly check recordings for suspicious activity ensuring at all times full compliance with the Data Protection Act 1998 which should be specified in your CCTV Data Protection Policy.

CCTV cameras should, if possible, cover entrances and exits to your institution and other areas that are critical to the safe management and security of your operation.

Ask yourself the following questions:

- Is your CCTV system currently achieving what you require it to do? Do you need it to confirm alarms, detect intruders through doors or corridors and produce images of evidential quality?
- Are the CCTV cameras in use for the protective security of your institution integrated with those used to monitor student or visitor movement?

Consider also the following points:

- Ensure the date and time stamps of the system are accurate.
- Regularly check the quality of recordings.
- Digital CCTV images should be stored in accordance with the evidential needs of the Police. Refer to CAST (HOSBD) publication 09/05.
- Ensure that appropriate lighting complements the system during daytime and darkness hours.

CCTV GUIDANCE

- keep any recorded images for at least 31 days
- Use good quality media and check it regularly by checking that backups are operating correctly.
- Ensure the images recorded are clear – that people and vehicles are clearly identifiable.
- Check that the images captured are of the right area.
- Implement standard operating procedures, codes of practice, audit trails and signage.
- Give consideration to the number of camera images a single CCTV operator can effectively monitor at any one time.
- Do you have sufficient qualified staff to continue to monitor your CCTV system during an incident, evacuation or search?

For further information on CCTV GUIDANCE please see **www.cpni.gov.uk**

- CCTV

MAIL HANDLING

Institutions often receive a wide variety of deliveries. This offers an attractive route into premises for terrorists.

You should consider the need for a screening process at the mail handling site, whether at a temporary or permanent structure and consider the following:

Delivered Items:

Delivered items, which include letters, parcels, packages and anything delivered by post or courier, has been a commonly used terrorist device. A properly conducted risk assessment should give you a good idea of the likely threat to your institution and indicate precautions you need to take.

Delivered items may be explosive or incendiary (the two most likely kinds), or chemical, biological or radiological. Anyone receiving a suspicious delivery is unlikely to know which type it is, so procedures should cater for every eventuality.

Delivered items come in a variety of shapes and sizes; a well-made one will look innocuous but there may be tell-tale signs.

Indicators to Suspicious Deliveries/Mail:

- It is unexpected or of unusual origin or from an unfamiliar sender.
- It is addressed to someone who may be at a higher risk than others: a high-profile member of the academic or research staff or the senior management team for instance.
- There is no return address or the address cannot be verified.
- It is poorly or inaccurately addressed e.g. incorrect title, spelt wrongly, title but no name, or addressed to an individual no longer with the company.
- The address has been printed unevenly or in an unusual way.
- The writing is in an unfamiliar or unusual style.
- There are unusual postmarks or postage paid marks.
- A Jiffy bag, or similar padded envelope, has been used.
- It seems unusually heavy for its size. Most letters weigh up to about 28g or 1 ounce, whereas most effective letter bombs weigh 50–100g and are 5mm or more thick.
- It is marked 'personal' or 'confidential'.
- It is oddly shaped or lopsided.
- The envelope flap is stuck down completely (a harmless letter usually has an ungummed gap of 3–5mm at the corners).
- There is an unusual smell, particularly of bleach, almonds or marzipan.
- There is an additional inner envelope, and it is tightly taped or tied (however, in some organisations sensitive or 'restricted' material is sent in double envelopes as standard procedure).

SEARCH PLANNING

Consider searches as part of your daily good housekeeping routine. They should also be conducted in response to a specific threat and when there is a heightened response level.

As previously mentioned under Security Planning, it is recognised that for the majority of institutions responsibility for the implementation of any search planning, following a vulnerability and risk assessment, will fall upon the Security Manager.

The following advice is generic for most institutions, if considered necessary, advice and guidance on searching should be available through your local Police Security Co-ordinator (SecCo) if appointed, CTSA or Police Search Advisor (PolSA).

Search Plans

- Search plans should be prepared in advance and staff should be trained.
- The conduct of searches will depend on local circumstances and local knowledge, but the overall objective is to make sure that the entire area, including grounds, are searched in a systematic and thorough manner so that no part is left unchecked.
- If you decide to evacuate in response to an incident or threat, you will also need to search it in order to ensure it is safe for re-occupancy.
- The police will not normally search premises. They are not familiar with the layout and will not be aware of what should be there and what is out of place. They cannot, therefore, search as quickly or as thoroughly as a member of staff or on site security personnel.
- The member(s) of staff nominated to carry out the search do not need to have expertise in explosives or other types of device. But they must be familiar with the place they are searching. They are looking for any items that should not be there, that cannot be accounted for and items that are out of place.
- Ideally, searchers should search in pairs; to ensure searching is systematic and thorough.

Action You Should Take

Consider dividing your institution area into sectors. If the site is organised into areas and sections, these should be identified as separate search sectors. Each sector must be of manageable size.

The sectored search plan should have a written checklist – signed when completed – for the information of the Security Manager.

Remember to include any stairs, fire escapes, corridors, toilets and lifts in the search plan, as well as car parks, service yards and other areas outside. If evacuation is considered or implemented, then a search of the assembly areas, the routes to them and the surrounding area should also be made prior to evacuation.

Exercise your search plan regularly. The searchers need to get a feel for the logical progression through their designated area and the length of time this will take. They also need to be able to search without unduly alarming any visitors.

For further information on SEARCH PLANNING' please see **www.cpni.gov.uk**

- Building and Area Search'

EVACUATION

As with search planning, evacuation should be part of your security plan. You might need to evacuate your institution because of:

- A threat received directly to the institution management.
- A threat received elsewhere and passed on to you by the police.
- Discovery of a suspicious item (perhaps a postal package, an unclaimed hold-all or rucksack).
- Discovery of a suspicious item or vehicle outside the establishment.
- An incident to which the police have alerted you.

Whatever the circumstances, you should tell the police as soon as possible what action you are taking.

The biggest dilemma facing anyone responsible for an evacuation plan is how to judge where the safest place might be. For example, if an evacuation route takes people past a suspect device outside your building, or through an area believed to be contaminated, external evacuation may not be the best course of action.

A very important consideration when planning evacuation routes in response to near simultaneous terrorist attacks is to ensure people are moved away from other potential areas of vulnerability, or areas where a larger secondary device could detonate.

The decision to evacuate will normally be yours, but the police will advise. In exceptional cases they may insist on evacuation, although they should always do so in consultation with your Security Manager.

A general rule of thumb is to find out if the device is external or internal to any premises or buildings. If it is within a building you may consider evacuation, but if the device is outside the building it may be safer to stay inside.

Planning and initiating evacuation should be the responsibility of the Security Manager. Depending on the size of your institution and the location of the building, the plan may include:

- Full evacuation outside the premises or building.
- Evacuation of part of the premises or building, if the device is small and thought to be confined to one location (e.g. a small bag found in an area easily contained).
- Full or partial evacuation to an internal safe area, such as a protected space, if available.
- Evacuation of all staff apart from designated searchers.

Evacuation instructions must be clearly communicated to staff and routes and exits must be well defined. Appoint people to act as marshals and as contacts once the assembly area is reached. Assembly areas should be a minimum of 100, 200 or 400metres away dependent upon the size of the item. Care should be taken that there are no secondary hazards at the assembly point.

It is important to ensure that staff are aware of the locations of assembly areas for incident evacuation as well as those for fire evacuation and that the two are not confused by those responsible for directing members of the public to either.

EVACUATION

Car parks should not be used as assembly areas and furthermore assembly areas should always be searched before they are utilised.

Staff, students and visitors with disabilities should be individually briefed on their evacuation procedures, and liaise with the institution to develop their own Personal Emergency Evacuation Plans (PEEPS).

DYNAMIC LOCKDOWN

Lockdown procedures should be seen as a sensible and proportionate response to any external or internal incident which has the potential to pose a threat to the safety of staff and pupils in the school. Procedures should aim to minimise disruption to the learning environment whilst ensuring the safety of all pupils and staff.

Lockdown arrangements should be determined by schools on an individual basis, as they will be dependent to a large extent on local circumstances such as premises design and layout, class arrangements, resources available, etc.

What is dynamic lockdown?

Dynamic lockdown is the ability to quickly restrict access and egress to a site or building (or part of) through physical measures in response to a threat, either external or internal. The aim of lockdown is to prevent people moving into danger areas and preventing or frustrating the attackers accessing a site (or part of). It is recognised that due to their nature some sites may not be able to physically achieve lockdown.

Why develop dynamic lockdown?

Those seeking to conduct attacks often undertake a level of planning including hostile reconnaissance. All opportunities to detect and deter threats at the attack planning phase should be taken. Presenting a strong security posture through visible and effective activity, for example by staff awareness and reporting processes, efficient use of CCTV, deterrent communications and active security zones.

If preventing an attack has not been possible, the ability to frustrate and delay the attacker(s) during the course of the attack and reduce the number of potential casualties can be greatly increased through dynamic lockdown.

Advance planning of what needs to be done to lockdown a site and recognising the need for flexibility in those plans will save lives.

Planning should consider:

- How to achieve effective full or partial lockdown
- How to let people know what's happening
- Training your staff
- STAY SAFE principles

"Stay Safe" is a short film capturing the actions that people should take in the event of a firearms or weapons attack.

It contains the main messages of **RUN > HIDE > TELL**

DYNAMIC LOCKDOWN

How to achieve dynamic lockdown

In your planning you should identify all access and egress points in both public and private areas of the site. Remember, access points may be more than just doors and gates.

- Identify how to quickly and physically secure access/egress points
- Identify how your site can be sectored to allow specific areas to be locked down
- Staff roles and responsibilities should be included in the plans.
- Staff must be trained to act effectively and made aware of their responsibilities
- Stopping people leaving or entering the site – direct people away from danger
- Ability to disable lifts without returning them to the ground floor should be considered
- Processes need to be flexible enough to cope with and compliment invacuation and evacuation

Two types of Lockdown

Schools should consider having two types of lockdown; 'partial' and 'full'.

1. Partial Lockdown

Alert to staff: 'Partial lockdown'

In a partial lockdown staff and pupils should remain in the school building and all doors leading outside should be locked. No one should be allowed to enter or leave the building; however teaching and work can continue as usual. This may be as a result of a reported incident / civil disturbance in the local community with the potential to pose a risk to staff and pupils in the school. It may also be as a result of a warning being received regarding the risk of air pollution, etc.

Immediate action:

- All outside activity to cease immediately, pupils and staff return to building. (There needs to be a means of communicating the alert to duty staff at break times).
- All staff and pupils remain in building and external doors and windows locked.
- Free movement may be permitted within the building dependent upon circumstances.
- In the event of an air pollution or chemical, biological or radiological contaminants issue, air vents, fans, heating and air conditioning systems should be closed or turned off.
- Use anything to hand to seal up all the cracks around doors and any vents into the room – you aim to minimise possible ingress of pollutants.
- Staff should await further instructions

2. Full Lockdown

Alert to staff: 'Full lockdown'

This signifies an immediate threat to the school and may be an escalation of a partial lockdown. The aim of a full lockdown is for the school and its rooms to appear empty.

Immediate action:

- All pupils/staff stay in their classroom or move to the nearest classroom.
- Office staff should remain in their office.

DYNAMIC LOCKDOWN

- External doors locked. Classroom doors locked (where a member of staff with key is present).
- Windows locked, blinds drawn, internal door windows covered (so an intruder cannot see in).
- Pupils/staff sit quietly out of sight and where possible in a location that would protect them from gunfire (bullets go through glass, brick, wood and metal. Consider locations behind substantial brickwork or heavy reinforced walls).
- Lights, smartboards and computer monitors turned off.
- Mobile phones turned off (or at the least turned onto silent so they cannot give away your position).
- A register to be taken of all pupils/staff in each classroom/office.
- Communicate register of staff/pupils to a pre-agreed central office.
- Staff should await further instructions.

Staff and pupils remain in lock down until it has been lifted by a senior member of staff/emergency services. At any point during the lockdown, the fire alarm may sound which is a cue to evacuate the building.

During the lockdown, staff will keep agreed lines of communication open but not make unnecessary calls to the central office as this could delay more important communication.

Examples of discreet communication channels might be:

- Where a school uses 'Parentmail' then staff could be put into a defined user group. This could then be used to communicate instructions via text message in an emergency
- Where staff have access to an internal e-mail system, they could access their account and await further instruction. In practical terms, staff would need to be familiar with accessing their account through a variety of means eg laptop, smartphone or tablet.

Training your staff

Due to the fast moving nature of incidents that require lockdown it is important that all staff are able to act quickly and effectively.

- Train all staff using principles of "Stay Safe" (Annex A)
- Ensure people know what is expected of them, their roles and responsibilities
- Check staff understanding
- Regularly test and exercise plans with staff
- Regularly refresh training

For further advice and guidance please see NaCTSO Guidance Note 1/2015 page 34 – 36 of this document.

Note: Use of fire alarms should be avoided to reduce incorrect response to an incident.

LOCKDOWN PROCEDURE

Lockdown Procedure

This document contains an example of a Lock Down Procedure for your consideration. It is acknowledged that not all schools are the same and that a 'one size' procedure will not suit all schools.

Lockdown procedures should be seen as a sensible and proportionate response to any external or internal incident which has the potential to pose a threat to the safety of staff and pupils in the school. Procedures should aim to minimise disruption to the learning environment whilst ensuring the safety of all pupils and staff.

Lockdown procedures may be activated in response to any number of situations, but some of the more typical might be:

- A reported incident / civil disturbance in the local community (with the potential to pose a risk to staff and pupils in the school)
- An intruder on the school site (with the potential to pose a risk to staff and pupils)
- A warning being received regarding a risk locally, of air pollution (smoke plume, Gas cloud etc)
- A major fire in the vicinity of the school
- The close proximity of a dangerous dog roaming loose

The school's lockdown plan is as follows:

Signal for lockdown	Three short start-stop-start-stop bell rings on the fire alarm system
Signal for all clear	Verbally from staff member via classroom telephones and/or walk round
Rooms most suitable for lockdown	All classes to remain in own classrooms
Entrance points (e.g. doors, windows) which should be secured	External doors, Fire Doors, Internal doors, All windows
Communication arrangements	In person or classroom telephones

Lockdown Drill

Staff will be alerted to the activation of the lockdown drill in advance.

When the three start-stop-start-stop bell rings on the fire alarm system are activated staff must take the following action:

- Pupils who are outside of the school buildings are brought inside as quickly as possible and return to their classroom (outside staff will be informed by a senior member of staff)

LOCKDOWN PROCEDURE

- Those inside the school should remain in their classrooms and check corridors and toilets for pupils or staff
- All external doors and, as necessary, windows are closed (depending on the circumstances, internal classroom doors must also be closed).
- Blinds should be drawn and pupils sit quietly
- Once in lockdown mode, staff should notify the office immediately of any pupils not accounted for via the internal telephone system and instigate an immediate search for anyone missing
- Staff should encourage the pupils to keep calm
- As appropriate, the school office will establish communication with the Emergency Services
- If it is necessary to evacuate the building, the fire alarm will be sounded and the usual fire drill procedure will then take place
- Parents will be notified as soon as it is practicable via Parentmail and the website (only when appropriate via guidance from Emergency Services)

Pupils will not be released to parents during a lockdown.

It is of vital importance that the school's lockdown procedures are familiar to all members of the school staff. To achieve this, a lockdown drill should be undertaken at least once a year.

All situations are different, once all staff and pupils are safely inside, senior staff will conduct an on-going risk assessment based on advice from the Emergency Services. This can then be communicated to staff and pupils. Emergency Services will advise as to the best course of action in respect of the prevailing threat.

Lockdown Drill – All clear

Once the incident has been assessed as safe all classrooms will be either visited by a senior member of staff or via classroom telephone and told the situation is under control and the class can resume activities as normal.

Communication between parents and the school

In the event of an actual lockdown, any incident or development will be communicated to parents as soon as is practicable.

Emergency Services

It is important to keep lines of communication open with Emergency Services as they are best placed to offer advice as a situation unfolds. The school site may or may not be cordoned off by Emergency Services depending on the severity of the incident that has triggered the Lockdown.

Emergency Services will support the decision of the Headteacher with regarding the timing of communication to parents.

LOCKDOWN PROCEDURE

Staff will ALWAYS have advance notice of a Lockdown drill, therefore if the signal occurs without warning staff must assume it is **NOT A DRILL.**

DRILL

SLT/Site Manager to sound 3 short blasts on the fire alarms in both buildings:

Infant building: person who rings the bell will time from start to clearance of hall and corridors/toilets – They will note the time that it takes for all classes to be contained and in full Lockdown.

Junior Building: person who rings the bell will time from start to clearance of hall and corridors/toilets – They will note the time that it takes for all classes to be contained and in full Lockdown.

Duties/Check List

Headteacher/Deputy Headteacher must ensure the following procedures take place:

Jobs	Checked
Allocate a member of staff to go outside and check playground and fields and tell those outside to return to their classrooms as Lockdown Drill is taking place.	
Office Staff member to take calls from classrooms if teachers report missing persons.	
Allocate Infant Bell Ringer: This person must ring office once the lockdown is complete to give the all clear.	
Verbally/or telephone all classes to inform staff that Lockdown is over.	
Allocate Junior Bell Ringer: This person must go to the office once the lockdown is complete to give the all clear.	
Verbally/or telephone all classes to inform staff that Lockdown is over.	

Pupils will not be released to parents during a lockdown.

It is of vital importance that the school's lockdown procedures are familiar to all members of the school staff. To achieve this, a lockdown drill should be undertaken at least once a year.

All situations are different, one all staff and pupils are safely inside, senior staff will conduct an on – going risk assessment based on advice from the Emergency Services. This can then be communicated to staff and pupils. Emergency Services will advise as to the best course of action in respect of the prevailing threat.

Lockdown Drill – All clear

Once the incident has been assessed as safe all classrooms will be either visited by a senior member of staff or via classrooms telephone and told the situation is under control and the class can resume activities as normal.

LOCKDOWN PROCEDURE

Communication between parents and the school
In the event of an actual lockdown, any incident or development will be communicated to parents as soon as practicable.

Emergency Services

It is important to keep lines of communication open with Emergency Services as they are best placed to offer advice as a situation unfolds. The school site may or may not be cordoned off by Emergency Services depending on the severity of the incident that has triggered the Lockdown.

Emergency Services will support the decision of the Head teacher regarding the timing of communication to parents.

Staff will always have advance notice of a Lockdown drill, therefor it the signal occurs without warning staff must assume it is NOT A DRILL.

STAY SAFE

Firearms and weapons attack

'Stay Safe' principles (Run Hide Tell) give some simple actions to consider at an incident and the information that armed officers may need in the event of a firearms and weapons attack. Full guidance is contained on the NaCTSO website https://www.gov.uk/government/publications/recognising-the-terrorist-threat

RUN

- Escape if you can.
- Consider the safest options.
- Is there a safe route? RUN if not HIDE.
- Can you get there without exposing yourself to greater danger?
- Insist others leave with you.
- Leave belongings behind.

HIDE

- If you can't RUN, HIDE.
- Find cover from gunfire.
- If you can see the attacker, they may be able to see you.
- Cover from view does not mean you are safe, bullets go through glass, brick, wood and metal.
- Find cover from gunfire e.g. substantial brickwork / heavy reinforced walls.
- Be aware of your exits.
- Try not to get trapped.
- Be quiet, silence your phone.
- Lock / barricade yourself in.
- Move away from the door.

TELL

CALL 999 – What do the police need to know?

- **Location** – Where are the suspects?
- **Direction** – Where did you last see the suspects?
- **Descriptions** – Describe the attacker, numbers, features, clothing, weapons etc.
- **Further information** – Casualties, type of injury, building information, entrances, exits, hostages etc.
- Stop other people entering

Armed Police Response

- Follow officers' instructions.
- Remain calm.
- Can you move to a safer area?
- Avoid sudden movements that may be considered a threat.
- Keep your hands in view.

Officers may

- Point guns at you.
- Treat you firmly.
- Question you.
- Be unable to distinguish you from the attacker.
- Officers will evacuate you when it is safe to do so.

You must STAY SAFE

- What are your plans if there were an incident?
- What are the local plans? e.g. personal emergency evacuation plan.

For further information on 'STAY SAFE' please see the sign post to web sites on Page 38 paragraph 4 of this document.

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT

1 Remain calm and talk to the caller
2 Note the caller's number if displayed on your phone
3 If the threat has been sent via email or social media see appropriate section below
4 If you are able to, record the call
5 Write down the exact wording of the threat:

WHEN WHERE
WHAT HOW
WHO WHY
TIME

ASK THESE QUESTIONS & RECORD ANSWERS AS ACCURATELY AS POSSIBLE:

1. Where exactly is the bomb right now?	
2. When is it going to explode?	
3. What does it look like?	
4. What does the bomb contain?	
5. How will it be detonated?	
6. Did you place the bomb? If not you, who did?	
7. What is your name?	
8. What is your address?	
9. What is your telephone number?	
10. Do you represent a group or are you acting alone?	
11. Why have you placed the bomb?	
Record time call completed:	

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT

INFORM BUILDING SECURITY/ COORDINATING MANAGER

Name and telephone number of person informed:

DIAL 999 AND INFORM POLICE Time informed:

This part should be completed once the caller has hung up and police/ building security/ coordinating manager have all been informed

Date and time of call: Duration of call:

The telephone number that received the call:

ABOUT THE CALLER: ☐ Male ☐ Female ☐ Age? Nationality

THREAT LANGUAGE:

☐ Well-spoken	☐ Irrational	☐ Taped
☐ Foul	☐ Incoherent	

CALLER'S VOICE:

☐ Calm	☐ Crying	☐ Clearing throat
☐ Angry	☐ Nasal	☐ Slurred
☐ Excited	☐ Stutter	☐ Disguised
☐ Slow	☐ Lisp	☐ *Accent
☐ Rapid	☐ Deep	☐ Familiar
☐ Laughter	☐ Hoarse	
☐ Other (please specify)		

What Accent?

If the voice sounded familiar, who did it sound like?

BACKGROUND SOUNDS:

☐ Street noises	☐ House noises	☐ Animal noises	☐ Crockery
☐ Clear	☐ Voice	☐ Static	☐ PA system
☐ Booth	☐ Factory machinery	☐ Office machinery	☐ Music

☐ Other (please specify)

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT

REMARKS:

ADDITIONAL NOTES:

Signature: Print Name: Date:

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT SENT VIA EMAIL OR SOCIAL MEDIA

1 **DO NOT** reply to, forward or delete the message

2 If sent via email note the address

3 If sent via social media what application has been used and what is the username/ID?

4 Dial **999** and follow police guidance

5 Preserve all web log files for your organisations to help the police investigation (as a guide, 7 days prior to the threat message and 48 hours after)

Signature: Print Name: Date:

SAVE AND PRINT – HAND COPY TO POLICE AND SECURITY/ COORDINATING MANAGER

Retention Period: 7 years
MP 925/10

NACTSO GUIDANCE NOTE 1/2015 DEVELOPING

NaCTSO
National Counter Terrorism Security Office

NPCC
National Police Chiefs' Council
National Counter Terrorism

Dynamic Lockdown Procedures

This note provides guidance to develop procedures to dynamically lockdown their sites in response to a fast moving incident such as a firearms or weapons attack, either directly at the site or in the vicinity. Due to the differences between the vast array of sites in the UK it is not possible to give prescriptive advice, however this guidance details planning considerations applicable to most sites.

What is dynamic lockdown?

Dynamic lockdown is the ability to quickly restrict access and egress to a site or building (or part of) through physical measures in response to a threat, either external or internal. The aim of lockdown is to prevent people moving into danger areas and preventing or frustrating the attackers accessing a site (or part of). It is recognised that due to their nature some sites may not be able to physically achieve lockdown.

Why develop dynamic lockdown?

Those seeking to conduct attacks often undertake a level of planning including hostile reconnaissance. All opportunities to detect and deter threats at the attack planning phase should be taken. Presenting a strong security posture through visible and effective activity, for example by staff awareness and reporting processes, efficient use of CCTV, deterrent communications and active security zones.

In preventing an attack has not been possible, the ability to frustrate and delay the attacker(s) during the course of the attack and reduce the number of potential casualties can be greatly increased through dynamic lockdown.

Advance planning of what needs to be done to lockdown a site and recognising the need for flexibility in those plans will save lives.

Planning should consider:

- How to achieve effective full or partial lockdown
- How to let people know what's happening
- Training your staff
- STAY SAFE principles

How to achieve dynamic lockdown:

- In your planning you should identify all access and egress points in both public and private areas of the site. Remember, access points may be more than just doors and gates.
- Identify how to quickly and physically secure access/egress points
- Identify how your site can be sectored to allow specific areas to be locked down

NACTSO GUIDANCE NOTE 1/2015 DEVELOPING

- Staff roles and responsibilities should be included in the plans.
- Staff must be trained to act effectively and made aware of their responsibilities
- Stopping people leaving or entering the site – direct people away from danger
- Ability to disable lifts without returning them to the ground floor should be considered
- Processes need to be flexible enough to cope with and compliment invacuation and evacuation

How to let people know what's happening

Various options exist depending on the nature and occupancy of the site, these include:

- Public Address (PA) system
- Existing internal messaging systems; text, email, staff phones etc.
- "Pop up" on employees computers / internal messaging systems
- Dedicated "Lockdown" alarm tone
- Word of mouth

For multi occupancy sites, methods of communication between all businesses need to be considered. Likewise, working with surrounding businesses will not only benefit situational awareness but build effective lines of communication.

Note: Use of fire alarms should be avoided to reduce incorrect response to an incident. Training your staff

Due to the fast moving nature of incidents that require lockdown it is important that all staff are able to act quickly and effectively.

- Train all staff using principles of "Stay Safe"
- Ensure people know what is expected of them, their roles and responsibilities
- Check staff understanding
- Regularly test and exercise plans with staff
- Regularly refresh training

For further advice and guidance please visit the NaCTSO website:
www.nactso.gov.uk

NACTSO GUIDANCE NOTE 1A/2016

NaCTSO
National Counter Terrorism Security Office

NPCC
National Police Chiefs' Council
National Counter Terrorism

Advice to leaders of schools and other Educational Establishments for Reviewing Protective Security

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

Consider what steps you could take to:

a) reassure your staff, students and parents

b) review and implement proportionate protect and prepare security planning.

1. Bomb threats:
Procedures for handling bomb threats. Most bomb threats are made over the phone and the overwhelming majority are hoaxes, made with the intent of causing alarm and disruption. Any hoax is a crime and, no matter how ridiculous or unconvincing, must be reported to the police.

Dial 999 and police will respond. You should always consider their advice before a decision is taken to close or evacuate.

Guidance on receipt of a bomb threat
http://www.cpni.gov.uk/security-planning/business-continuity-plan/bomb-threats/

Bomb threat checklist
http://www.cpni.gov.uk/documents/posters%20and%20checklists/bomb-threat-checklist.pdf?epslanguage=en-gb

If this prompts you to review your emergency planning, consider the following:

2. Search Planning:
Do you have plans to search your site to deal effectively with either bomb threats or for secreted threat items; are your staff and students familiar with those plans and what to do if they find a suspicious item?

Good housekeeping reduces the opportunity for suspicious items to be placed and assists effective search.

Security guidance for educational establishments
https://www.gov.uk/government/publications/counter-terrorism-protective-security-advice-for-higher-and-further-education

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

NACTSO GUIDANCE NOTE 1A/2016

3. Evacuation/Invacuation planning: It is vital that you are able to move your staff and students away from danger in a controlled way. Ensure you have a number of options available, well sign-posted and notified to people on your site. Keep routes clear.

Sometimes it may be safer to remain inside a building; identify the most suitable internal spaces that staff and students can move to.

Security guidance for educational establishments

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

Evacuation Planning

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

4. STAY SAFE Guidance for firearms and weapons attacks:

Do your staff follow the Stay Safe principles RUN HIDE TELL?

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

Stay safe film

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

Dynamic lockdown guidance

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

5. Staff Awareness & Security Culture: Have you briefed your staff on how they can recognise suspicious activity?

Employee vigilance

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

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

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

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

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

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

8. Mail handling: a threat may still exist from items delivered to your establishment by hand or by post. Are your staff familiar with indicators for suspicious deliveries?

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

9. Further advice: is available at: https://www.gov.uk/guidance/emergencies-and-severe-weather-schools-and-early-years-settings

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

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

NACTSO GUIDANCE NOTE 8/2016

NaCTSO
National Counter Terrorism Security Office

NPCC
National Police Chiefs' Council
National Counter Terrorism

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

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

Consider what steps you could take to:

c) reassure your staff, students and parents

d) review and implement proportionate protect and prepare security planning

1. Bomb threats: Procedures for handling bomb threats.

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

1.1 The bomb threat message.

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

1.2 Communication of the threat.

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

noted that a threat may be communicated via a third-party, i.e. a person or organisation unrelated to the intended victim.

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

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

If you receive a telephone threat you should:

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

If the threat is delivered face-to-face:

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

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

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

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

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

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

1.4 The Credibility of Bomb Threats.

Evaluating the credibility of a threat is a critical task, particularly if the attack being threatened is imminent. This is a tactic used to place additional pressure on decision makers.

When specific intelligence is known to police, advice will be issued accordingly; however, in the absence of information, it will be necessary to consider a number of factors:

- is the threat part of a series? If so, what has happened elsewhere or previously?

- can the location of the claimed bomb(s) be known with precision? If so, is a bomb visible at the location identified?
- considering the hoaxer's desire to influence behaviour, is there any reason to believe their words?
- if the threat is imprecise, could an external evacuation inadvertently move people closer to the hazard?

2. Evacuation considerations.

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

2.1 External evacuation.

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

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

Minimum police cordon distances are:

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

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

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

2.2 Internal or inwards evacuation (invacuation).

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

2.3 No action.

This will be reasonable and proportionate if, after the evaluation by the venue, the threat is deemed

implausible or a hoax. Police may provide additional advice and guidance. A proportionate search of the venue should be considered.

Remember: it is vital that regular drills are carried out to ensure all are familiar with bomb threat procedures, routes and rendezvous points. Disabled staff should have personal evacuation plans and be individually briefed on their evacuation procedures. Similarly all visitors should be briefed on evacuation procedures and quickly identified and assisted in the event of a threat.

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

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

3. Search Considerations.

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

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

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

NACTSO GUIDANCE NOTE 8/2016

4. Media and Communication.

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

Releasing details of the circumstances may:

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

5. Firearms and Weapons Attacks.

RUN HIDE TELL

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

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

6. Dynamic Lockdown Guidance.

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

7. Staff Awareness and Security Culture.

Have you briefed your staff on how they can recognise suspicious activity? Consider an employee vigilance campaign

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

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

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

8. Physical Security.

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

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

9. Mail Handling.

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

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

10. Security Guidance for Educational Establishments.

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

11. Emergency Planning and Response Advice.

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

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

NOTES

NOTES

REF: 2490-18 Designed and Printed by South Wales Police Print Department.