Counter Terrorism Protective Security Advice For Schools

Foreword

This guidance has been developed with advice from the National Counter Terrorism Security Office to assist schools in addressing security issues relating to the terrorist threat. The sheer range and scale of threats today mean that we have to be more pro-active in our measures to reduce the vulnerability of our organisations, our people, and our sites.

The law requires all schools to carry out adequate risk assessments and ensure that suitable measures are in place to manage ALL identified risks. Prompt and regular reviews of those assessments and measures, **in light of new threats and developments including terrorism and extreme violence**, should be conducted.

Equally important is that business continuity plans address security issues, to ensure that schools can cope with an incident, and return to 'business as usual' as soon as possible. Having a robust security culture and being better prepared reassures the whole school community that you are taking security issues seriously.

Governing Bodies and Senior Management should bring this guidance to the attention of all relevant staff. These are likely to include Teaching Staff, Site and Security Management, Facilities, and Health & Safety.

Although each school will have its own particular circumstances, this guidance addresses all of the areas of concern and includes useful Good Practice checklists to ensure that all the risks immediately visible. This is followed by more comprehensive guidance for schools to further develop their knowledge and procedures.

The need to focus on proper preparation and prevention to guard against criminal prosecution for safety and security lapses has sharpened with the introduction of legislation which gives the courts power to send individual directors, managers and others to jail for up to 2 years for a breach of health and safety duties. Previous legislation provided only for a fine. See Corporate Manslaughter Act 2008 and Corporate Homicide Act 2007.

Emergency and business continuity planning

Your business continuity strategy is essential in ensuring that schools can simultaneously respond to an incident and return to 'business as usual' as soon as possible. You have already developed an emergency response plan, which should cover a wide range of possible situations, and preparing for a terrorist incident or extreme violence should link in with this.

This guide recognises that schools differ in many ways including size, location, layout and operation and that some of the advice included in this document may already have been introduced. The good practice checklists included at the forefront can be used as a 'health check' for schools and are no replacement for specialised advice. Comprehensive guidance is developed further in the document, as well as contact details for further resources and help.

It is essential that all the work you undertake on protective security is undertaken in partnership with the local authority school security specialist and trustees/governors as appropriate, if your premises are to be secure.

It is worth remembering that measures you have already considered for other threats, such as theft and criminal damage, help against countering terrorism. Any extra measures that are considered should integrate wherever possible with existing security.

Introduction

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

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. **Guidance on Information Security is already covered in your E Safety Policy**, **and your responsibilities under the Data Protection Act.**

Some attacks are easier to carry out if the terrorist is assisted by an 'insider' or by someone with specialist knowledge or access. **Guidance on Personnel Security is already covered in your Safe Recruitment Policy and Practices.**

It is possible that educational facilities could be the target of a terrorist incident, or your school could be located near one. You may have to deal with a bomb threat locally or suspect items left in or around premises near school, and the impact of this would be dealing with the consequences, such as evacuation, communication and transport issues.

This advice serves to inform rather than alarm. 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.

Law, Liability and Insurance

There are legal and commercial reasons why security plans should deter such acts, or at least minimise their impact. Adequate cover for loss of revenue and business interruption during a rebuild or repair is expensive - *where available from the limited pool of specialist underwriters*. Full protection against compensation claims for death and injury to staff and customers caused by terrorism is achievable, albeit at a cost.

With individual awards for death and serious injury commonly exceeding the publicly-funded criminal injuries compensation scheme upper limit, there is every incentive for victims to seek to make up any shortfall through direct legal action against owners, operators, managers and tenants under occupier's liability laws. Having to pay large and numerous compensation claims out of your own uninsured pocket could have a high impact on your organisation.

Criminal prosecution and heavy penalties under health and safety laws for bodies and individuals who manage or are responsible for schools are a real possibility in the wake of a terrorist incident, *particularly if it emerges that core standards and statutory duties have not been met*.

Particularly relevant to protective security are the specific requirements of the Health and Safety at Work Act 1974 and Regulations made under it to do all of the following:

- **Carry out adequate risk assessments** and put suitable measures in place to manage identified risks, even where they are not of the institution's making and are outside their direct control: then be alert to the need to conduct prompt and regular reviews of those assessments and measures in light of new threats and developments
- **Co-operate and co-ordinate** safety arrangements between governors, senior management, teaching and site staff, tenants (i.e. breakfast/holiday clubs etc.) and others involved on site, including the sharing of incident plans and working together in testing, auditing and improving planning and response
- **Ensure adequate training, information and equipment** are provided to all staff, and especially to those involved directly with safety and security
- Put proper procedures and competent staff in place to deal with **imminent and serious danger** and evacuation.

Part 1 - Good practice checklists

The following checklists are intended as a health check to help to immediately identify the hazards and risks associated with counter terrorism planning, which should link in with your existing Emergency Plan.

They are not exhaustive and some of the guidance might not be relevant to all schools.

Having completed the various 'Good Practice' checklists you need to give further attention to the questions that you have answered 'no' or 'Unsure' to.

If you answered 'Unsure' to a question, find out more about that particular issue to reassure yourself that this vulnerability is being addressed or needs to be addressed.

If you answered 'no' to any question then you should seek to address that particular issue as soon as possible.

Where you have answered 'yes' to a question, remember to regularly review your security needs to make sure that your security measures are fit for that purpose.

IT SHOULD BE REMEMBERED THAT ONE OF THE GREATEST THREATS TO ANY ORGANISATION IS COMPLACENCY.

Emergency and Business Continuity Planning Health Check	**YES**	**NO**	**UNSURE**
		seek further guidance	seek further guidance
Do you have an Emergency Response and Business Continuity Plan?			
Do you regularly review and update your plans?			
Is counter terrorism or extreme violence/weapons attacks included as a hazard?			
Do you have sufficient insurance to pay for disruption to business, cost of repairs, hiring temporary employees, leasing temporary accommodation and equipment?			
Have you done a recent Fire Risk Assessment?			
Have you prepared an Emergency Grab Bag?			
Are essential contact numbers accessible remotely?			
Do you have a review process for updating plans as required?			

Housekeeping Good Practice	**YES**	**NO**	**UNSURE**
		seek further guidance	seek further guidance
Do you keep external areas, entrances, exits, stairs, reception areas and toilets clean and tidy?			
Do you keep furniture in public areas to a minimum to provide little opportunity to hide devices?			
Are unused classrooms, offices, meeting rooms, multi-purpose spaces locked or secured?			
Are your office and administration staff trained and competent in managing telephoned bomb threats?			
Have you reviewed the use and location of bins in external areas?			

Access Control Health Check	YES	NO	UNSURE
		seek further guidance	seek further guidance
Do you only allow staff, pre-arranged visitors and authorised delivery vehicles to park on site?			
Is there a clear demarcation identifying the public and private areas of your school?			
Do your staff, including contractors, cleaners and all other employees wear visible ID badges at all times when on site?			
Do you adopt a 'challenge culture' to anybody not wearing a pass in your private areas?			
Do all visitors have to report to reception before entry, are they required to sign in and issued with a visitors pass?			
Do visitors' badges look different from staff badges?			
Are visitors' badges collected from visitors when they leave?			
Are all visitors accompanied by staff at all times whilst in private areas?			

CCTV	YES	NO	UNSURE
		seek further guidance	seek further guidance
Is your CCTV monitored by a Control Room out of hours?			
Do you have your CCTV cameras regularly maintained and cleaned?			
Do the cameras cover the entrances and exits to your school?			
Do you have cameras covering critical areas such as server rooms, specialist ICT equipment, back-up generators or restricted areas?			
Do you store the CCTV images in accordance with the evidential needs of the police?			
Could you positively identify an individual from the recorded CCTV images?			
Are the date and time stamps of the system accurate?			
Is each CCTV camera doing what it was installed to do?			

Evacuation/Invacuation	**YES**	**NO**	**UNSURE**
		seek further guidance	seek further guidance
Is evacuation part of your Emergency or Security Plan?			
Is invacuation into a protected space *within your site* part of your Emergency or Security Plan?			
Do you have nominated Evacuation/Invacuation Marshals, similar to the duties carried out by a Fire Marshal?			
Have you determined evacuation routes?			
Have you identified any spaces where people could be confined in the event of an emergency (Invacuation)?			
Do you have reliable, tested communications facilities in the event of an incident?			
Have any disabled or vulnerable staff been individually briefed about what would happen in the event of an incident? THINK about PEEP as part of EP and FIRE procedures.			

Personnel Security – Identity Assurance	**YES**	**NO**	**UNSURE**
		seek further guidance	seek further guidance
Would your current procedures for safe recruitment ensure that you could be assured of the identity of an individual?			
REFER TO YOUR EXISTING PROCEDURES			
Information Security			
Have you got an up to date Data Protection Policy and relevant registration with the Information Commissioner?			
Are your paper documents and files locked away at the end of the day?			
Have you got an up to date E Safety Policy which ensures correct protection of electronic information.			
REFER TO YOUR EXISTING PROCEDURES			

Communication	**YES**	**NO**	**UNSURE**
		seek further guidance	seek further guidance
Are security and emergency issues and concerns discussed/decided at senior management level and form a part of your school's culture?			
Do you have an up to date security policy, or other documentation showing how security procedures should operate within your school?			
Do you regularly meet with staff to discuss security issues?			
Do you encourage staff and/or pupils to raise concerns about security?			

Security during Events	YES	NO	UNSURE
		seek further guidance	seek further guidance
Do you consider extra security measures for events, such as parents evening or performances etc?			
Do you have separate security arrangements and procedures to ensure the safety of people on the premises during such events?			
Do you have special arrangements for evacuation or invacuation during these events?			
Is the site 'zoned' and restricted areas managed accordingly during events where members of the public are on the premises?			

Part 2 – Further guidance

Managing the risks

Managing the risk of terrorism or extreme violence is only one part of a school's responsibility when preparing plans in response to any incident which might prejudice personal safety or disrupt normal operations.

With regard to protective security, the best way to manage the risks to your institution 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 school 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:

Step One: Identify the threats.

Understanding the terrorists' intentions and capabilities - what they might do and how they might do it - is crucial to assessing threat. Ask yourself the following questions:

What can be learnt from the government and media about the current security climate, or about recent terrorist activities? Visit www.cpni.gov.uk

Is there anything about the location of your school, its visitors, sponsors, contractors, occupiers, pupils and staff, or your activities, that would particularly attract a terrorist attack?

Is there an association with high profile individuals or organisations which might be terrorist targets?

Do you have procedures in place and available for deployment on occasions should VIPs attend your institution?

Could collateral damage occur from an attack on a neighbouring premises or venue?

What can your local Police Service tell you about crime and other problems in the area of the school?

Do you communicate information about the threat and response levels to your staff?

Step Two: Decide what you need to protect and identify your vulnerabilities.

Your priorities for protection should fall under the following categories:

People (staff, students, parents, contractors and visitors)

Physical assets (buildings, contents, equipment, plans and sensitive materials)

Information (electronic and paper data)

Processes (supply chains, critical procedures) - the actual operational process and essential services required to support it.

You know what is important to your school. **You should already have plans in place for dealing with fire, crime and emergencies,** and practiced measures to secure the estate, building and grounds**.** Procedures for assessing the integrity of those you employ or contract, protection from IT viruses and hackers, are covered in your existing Safe Recruitment Practices and E Safety measures.

Consider what others could find out about your vulnerabilities, such as:

Information about you, that is publicly available, e.g. on the internet or in public documents.

You should have measures in place to limit access into service areas and vehicle access control measures into goods and service area.

As with Step One, consider whether there is an aspect of your school that terrorists might want to exploit to aid or finance their work. If there is, how stringent are your checks on the people you recruit or on your contract personnel or volunteer base? Are your staff security conscious?

It is important that your staff can identify and know how to report suspicious activity. (See hostile reconnaissance section).

Step Three: Identify measures to reduce risk

An integrated approach to security is essential - physical security, information security and personnel security. There is little point investing in costly security measures if they can be easily undermined by a disaffected member of staff or by a lax recruitment process.

Remember, TERRORISM IS A CRIME. Many of the security precautions typically used to deter criminals are also effective against terrorists. So before you invest in additional security measures, review what you already have in place. You may already have a good security regime on which you can build.

If you do need additional security measures, then make them most cost-effective by careful planning wherever possible. If you are using an area or premises normally used for another purpose, work with the occupiers to produce an integrated security package. Even if organisations / businesses surrounding your school are not concerned about terrorist attacks, they will be concerned about general crime - and your security measures will help protect against crime as well as terrorism.

Staff may be unaware of existing security measures, or may have developed habits to circumvent them, e.g. short cuts through fire exits. Simply reinstating good basic security practices and regularly reviewing them will bring benefits at negligible cost.

Step Four: Review your security measures and rehearse and review security and contingency plans.

You should regularly exercise and revise your plans to ensure that they remain accurate, workable and current.

Make sure that your staff understand and accept the need for security measures and that security is seen as part of everyone's responsibility, not merely something for security experts or professionals. Make it easy for people to raise concerns or report observations.

Security planning

The security plan is part of a wider security strategy also comprising business continuity and emergency management.

Your security and emergency planning procedures should take terrorism into account. Any temporary construction and buildings should also be considered so that counter terrorism specifications, e.g. glazing and physical barriers can be factored in at the outset, taking into account any planning and safety regulations.

Security and business continuity strategies should already include responsibility for most if not all of the following key areas:

- The production of the security plan based on the risk assessment
- The formulation and maintenance of a search plan
- The formulation and maintenance of other contingency plans dealing with bomb threats, suspect packages, protected spaces and evacuation
- Liaising with the police, other emergency services and local authorities
- Arranging staff training and conducting briefings/debriefings
- Conducting regular reviews of the plans.

For independent and impartial **counter terrorism advice** that is site specific, you should establish contact with the local police Counter Terrorism Security Advisor (CTSA).

Your CTSA can:

- Help you assess the threat, both generally and specifically
- Give advice on physical security equipment and its particular application to the methods used by terrorists; The CTSA will be able to comment on its effectiveness as a deterrent, as protection and as an aid to post-incident investigation

Creating your Security Plan

The designated person responsible for site security should aim to produce a plan that has been fully exercised, and which is regularly audited to ensure that it is still current and workable.

Before you invest in additional security measures, review what is already in place, including known weaknesses such as blind spots in a CCTV system.

The local authority education security specialist can help you with this. Contact Deborah Borg on 0161 778 0131 or deborah.borg@salford.gov.uk

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/training staff 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
- Evacuation plans and details on securing the building in the event of a full evacuation
- Your business continuity plan
- A communications and media strategy which includes handling enquiries from concerned family and friends. [See specific section on communication]

Managers should also be familiar with the following advice:

- The Fire Safety Risk Assessment - 'Small and Medium Places of Assembly' and 'Large Places of Assembly' guidance documents. Available to download at www.gov.uk

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, pupils, 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 hard 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.

Physical security

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

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, should be already in place. 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) to CCTV, perimeter fencing, intruder alarms, computer security and lighting – most of which are already in place in our schools.

Specialist solutions, in particular, should be based on a thorough assessment and independent advice from a security professional - not least because you might otherwise invest in equipment which is ineffective, unnecessary and expensive.

Successful security measures require:

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

Action you should consider

Contact the Local Authority Educational Security Specialist at the start of the process. As well as advising you on physical security, they can direct you to professional bodies that regulate and oversee reputable suppliers.

Remember, you will need to ensure that all necessary regulations are met, such as planning permission, 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 existing security measures can be easily integrated within the plan. Build on what you already have.

Security awareness

The vigilance of all staff and contractors 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 school, not a waste of time.

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. *See hostile*

reconnaissance section. Training in emergency response plans should also be included in staff inductions.

Access control

Keep access points to a minimum and make sure the boundary between public and private areas is secure and clearly signed. Ensure there are appropriately trained and briefed staff to manage access control points, or alternatively invest in good quality access control systems, especially in restricted access areas.

Security passes

If an access control system is in place, insist that staff and students (if appropriate) wear their passes at all times and that the issuing is strictly controlled and regularly reviewed. Passes should include a photograph of the bearer. Visitors to private or restricted areas should be escorted and should wear clearly marked temporary passes, which must be returned on leaving. Anyone not displaying security passes in private or restricted areas should either be challenged or reported immediately to security or management.

Traffic and parking controls

The basic principle is to keep all vehicles other than staff cars at a safe distance. Those requiring essential access, i.e. deliveries and contractors, should be identified in advance and checked before being allowed onto the site. If possible, you should ensure that you have proper access control, careful landscaping, traffic-calming measures and robust, well-lit barriers or bollards. The measures you already have in place to restrict unauthorised parking by parents and staff will already help this.

For site specific advice and guidance you should contact your local authority Educational Security Specialist on 0161 778 0131 or deborah.borg@salford.gov.uk

Doors and windows

Good quality doors and windows on permanent structures are essential to ensure building security, advice on the appropriate standards can be obtained from your local authority.

If using a temporary building structure, a survey of the existing doors, windows and build materials could be made to identify any gaps in mitigating your own security vulnerabilities. External doors should be strong, well lit and fitted with good quality locks.

Doors that are not often used should be internally secured ensuring compliance with relevant fire safety regulations and their security monitored with an alarm system if possible.

As a minimum, accessible windows should be secured with good quality key operated locks.

Many casualties in urban terrorist attacks are caused by flying glass, especially in modern buildings and glazing protection is an important casualty reduction measure.

- Extensive research has been carried out on the effects of blast on glass. There are technologies that minimise shattering and casualties, as well as the costs of re-occupation.
- Anti-shatter film, which holds fragmented pieces of glass together, offers a relatively cheap and rapid improvement to existing glazing. If you are installing new windows, consider laminated glass, but before undertaking any improvements seek specialist advice through your police CTSA or visit www.cpni.gov.uk

Perimeter

The style and quality of perimeter security will depend on the risks and vulnerabilities identified in your security assessment. Most schools already have sufficient boundary treatment to protect the site. Any temporary fencing must adhere to health & safety legislation and fire regulations, remembering safety must always have priority over security.

Integrated security systems

Intruder alarms, CCTV and lighting are commonly used to deter crime, detect offenders and delay their actions. All these systems should be integrated so that they work together in an effective and coordinated manner.

Good housekeeping

Good housekeeping improves the general appearance of your school 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 around critical/vulnerable areas i.e. do not place litter bins next to or near glazing, support structures, 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 and location.
- The use of clear bags for waste disposal is a further alternative as it provides an easier opportunity for site staff to conduct an initial examination for suspicious items.
- Review the use and security of 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.
- 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.
- Pruning vegetation and trees, especially near entrances, will assist in surveillance and prevent concealment of any packages.

Additionally consider the following points:

Staff training in bomb threat handling procedures, or at least have ready access to instructions - and know where these are kept. (See bomb threat checklist and aide memoir).

If you have CCTV, review your system to ensure it has sufficient coverage.

Fire extinguishers should be appropriately marked and authorised for the locations in which they will be kept. Regular checks should be made to ensure that they have not been interfered with or replaced.

All safety and security systems should have an uninterrupted power supply (UPS) available which is regularly tested if it is identified that power loss would impact on the safety of the public.

Access control

Any lack of vigilance around pedestrian and vehicle entrances to your school affords anonymity to a potential terrorist.

There should be clear demarcation between public and private areas, with appropriate access control measures into and out of the private areas.

Risk assessment

Refer to 'managing the risks' and decide the level of security you require before planning your access control system.

Appearance

The access control system to your private or restricted areas and service yards/delivery areas is often the first impression of security made upon persons visiting your premises.

Ease of access

Examine the layout of your system. Ensure that your entry and exit procedures allow legitimate users to pass without undue effort and delay.

Ideally, adopt a photo ID card access control system which varies in appearance for the different levels of access across the site. Staff should be instructed what to examine when checking passes and this should be quality assured through testing.

Training

Ensure staff are fully aware of the role and operation of your access control system. Your installer should provide adequate system training.

System maintenance

Your installer should supply all relevant system documentation, e.g. log books and service schedules. Are you aware of the actions required on system breakdown? Do you have a satisfactory system maintenance agreement in place? Is there a contingency plan you can implement at a moment's notice should it fail?

Compliance

Your access control system should be compliant with:

- Equality Act 2010
- The Data Protection Act 1998
- The Human Rights Act 1998
- Regulatory Reform (Fire Safety) Order 2005
- Health and Safety Acts

Access control is only one important element of your overall security system.

REMEMBER

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

CCTV guidance

If you have a CCTV system you should monitor the images where possible i.e. passing attention in reception - 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 school and other areas that are critical to the safe management and security of your site.

- Use cameras to focus on the activities of particular people of interest either by controlling or directing cameras to their activities.
- Use recorded CCTV images to identify individuals or to investigate their activities.
- Wherever possible, ensure that all CCTV systems are integrated centrally through a single CCTV policy for your school.

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?

Using CCTV can help clarify whether a security alert is real and is often vital in post-incident investigations, but only if the images are good enough to identify what happened and be used in court.

External lighting provides an obvious means of deterrence as well as detection, but the impact of additional lighting on your neighbours should be taken into account to avoid complaints later on. If it is carefully designed and used, external lighting will improve the capabilities of CCTV systems.

Remember that CCTV is only effective if it is properly monitored, maintained and can provide an active response.

Additional CCTV guidance is readily available from deborah.borg@salford.gov.uk on request.

Consider also the following points:

- Ensure the date and time stamps of the system are accurate
- Regularly check the quality of recordings
- Ensure that appropriate lighting complements the system during both day and night
- 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

Digital CCTV images should be stored in accordance with the evidential needs of the Police as follows:

With regards to the retention of footage, the police prefer quality over quantity. The overall retention period should be dictated by what the system is designed to achieve, though it would be better to have good quality images over a 14-day period than poor ones over a 30-day period.

Procedures for recovery of recordings should already be set up as part of your CCTV Policy. E.g. staff should be trained and the CCTV system instruction manual should be readily available.

Acceptable Standard - this generally requires a resolution of 720x576 pixels at a real time frame rate of 25 frames per second. N.B. Both the camera and DVR/NVR must be capable of this – if the camera will only send low resolution images then it does not matter how high the resolution of the recording unit is. Your CCTV maintainer will help with this.

Identification – One of three levels of field of view. To identify an individual, the image must capture no less than 120% of the field of view (at least from the top of the individuals head to their knees). The remaining two levels of field of view are 'Overview' and 'Recognition', which whilst effective for observational purposes, are less likely to result in the identification of a person/offender.

The intelligent placement of cameras helps to provide clear facial identification of individuals.

CCTV Maintenance

CCTV maintenance must be planned and organised in advance and not carried out on an ad- hoc basis. If regular maintenance is not carried out, the system may eventually fail to meet its Operational Requirement.

What occurs if a system is not maintained?

- The system gets **DIRTY** causing poor usability
- **CONSUMABLES** wear causing poor performance
- Major parts **FAIL**
- **WEATHER** damage can cause incorrect coverage
- **DELIBERATE** damage/environmental changes can go undetected

Small deliveries by courier and mail handling

Schools often receive a wide variety of deliveries. This could offer an attractive route into the premises for terrorists.

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. See www.cpni.gov.uk

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 telltale signs as follows.

Indicators to Suspicious Deliveries/Mail

- It is unexpected or of unusual origin or from an unfamiliar sender
- 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 school
- 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

If a suspicious item is identified, follow these key steps:

1. **Do not touch suspicious items.**
2. **Move everyone away to a safe distance.**
3. **Prevent others from approaching.**
4. **Communicate safely to staff, pupils 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 hard cover.**

6. **Notify the police.**
7. **Ensure that whoever found the item or witnessed the incident remains on hand to brief the police.**

Chemical, biological or radiological materials in the post

Terrorists may seek to send chemical, biological or radiological materials in the post. It is difficult to provide a full list of possible CBR indicators because of the diverse nature of the materials. However, some of the more common and obvious are:

- Unexpected granular, crystalline or finely powdered material (of any colour and usually with the consistency of coffee, sugar or baking powder), loose or in a container.
- Unexpected sticky substances, sprays or vapours.
- Unexpected pieces of metal or plastic, such as discs, rods, small sheets or spheres.
- Strange smells, e.g. garlic, fish, fruit, mothballs, pepper. If you detect a smell, do not go on sniffing it. However, some CBR materials are odourless and tasteless.
- Stains or dampness on the packaging.
- Sudden onset of illness or irritation of skin, eyes or nose.

CBR devices containing finely ground powder or liquid may be hazardous without being opened.

What you can do:

- The precise nature of the incident (chemical, biological or radiological) may not be readily apparent. Keep your response plans general and wait for expert help from the emergency services.
- Review plans for protecting staff, pupils and visitors in the event of a terrorist threat or attack. Remember that evacuation may not be the best solution. You will need to be guided by the emergency services at that time.
- Plan for the shutdown of systems that may contribute to the movement of airborne hazards (e.g. computer equipment containing fans and air-conditioning units).
- Ensure that doors can be closed quickly if required.
- Examine the feasibility of emergency shutdown of air-handling systems and ensure that any such plans are well rehearsed.
- Where a hazard can be isolated by leaving the immediate area, do so as quickly as possible, closing doors and windows as you go.
- Move those directly affected by an incident to a safe location as close as possible to the scene of the incident, so as to minimise spread of contamination.
- Separate those directly affected by an incident from those not involved so as to minimise the risk of inadvertent cross-contamination.
- Ask people to remain in situ - though you cannot contain them against their will.

You do not need to make any special arrangements beyond normal first aid provision. The emergency services will take responsibility for treatment of casualties.

Planning your mail handling procedures

Although any suspect item should be taken seriously, remember that most will be false alarms, and a few may be hoaxes. Try to ensure that your procedures, while effective, are not needlessly disruptive. Take the following into account in your planning:

- Consider processing all incoming mail and deliveries at one point only. This should ideally be in an area that can easily be isolated and in which deliveries can be handled without taking them through other parts of the site.
- Ensure that all staff who handle mail are briefed and trained. Include reception staff and encourage regular correspondents to put their return address on each item.
- Ensure that all sources of incoming mail (e.g. Royal Mail, couriers, and hand delivery) are included in your screening process.
- Staff need to be aware of the usual pattern of deliveries and to be briefed of unusual occurrences. Train them to open post with letter openers (and with minimum movement), to keep hands away from noses and mouths and always to wash their hands afterwards. Staff should not blow into envelopes or shake them. Packages suspected of containing biological, chemical or radiological material should ideally be placed in a double sealed bag.
- Consider whether staff who handle post need protective equipment such as latex gloves (seek advice from a qualified health and safety expert).
- Make certain post opening areas can be promptly evacuated. Rehearse evacuation procedures and routes, which should include washing facilities in which contaminated staff could be isolated and treated.
- Staff responsible for mail handling should be made aware of the importance of isolation in reducing contamination.
- Prepare signs for display to staff in the event of a suspected or actual attack.

For more guidance on mail handling procedures see www.cpni.gov.uk

Search planning

Where possible, consider routine searches or sweeps as part of your daily good housekeeping schedule.

As previously mentioned under Security Planning, it is recognised that for the majority of schools, responsibility for the implementation of any search planning following a vulnerability and risk assessment, will fall upon the designated person responsible for security or FM Site Manager or Fire Marshals.

The following advice is generic for most schools, but recognises that they operate differently.

Search Plans

- Search plans should be prepared in advance and staff should be trained in them.
- 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 FM Site Manager.
- 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 school 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 sectorised search plan should have a written checklist - signed when completed - for the information of the Caretaker or FM 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 emergency assembly areas, the routes to them and the surrounding area should also be made prior to evacuation.

Consider the most effective method of initiating the search. You could:

- Send a message to the search teams over a public address system if you have one (the messages should be coded to avoid unnecessary disruption and alarm)
- Use personal radios or pagers.

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 distance.**
3. **Prevent others from approaching.**
4. **Communicate safely to staff, 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 hard cover.**
6. **Notify the police.**
7. **Ensure that whoever found the item or witnessed the incident remains on hand to brief the police.**

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.

Searching visitors and their belongings is an element of protective security that should be considered following specific intelligence or advice from Police.

Evacuation and invacuation planning

Evacuation should be part of your security plan. You might need to evacuate your school because of:

- **A threat received directly to the school 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 the Head Teacher.

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 Head Teacher.

Depending on the size of your school 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 (invacuation) if available.
- Evacuation of all staff apart from designated searchers.

Evacuation

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 400 metres 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.

'Grab Bags' should be available in key locations, which contain essential equipment and information. All relevant contact information, the staff involved, tenants and other site information should be contained in an easily accessible format.

For suggested 'Grab Bag' contents please refer to the supplied check list.

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, with developed Personal Emergency Evacuation Plans (PEEPS).

Letter or parcel bombs

If in the premises evacuate the room concerned and the adjacent rooms along. If the structures are of temporary construction i.e. modular cabins, then evacuate at least 100, 200 or 400 metres dependent upon the size of the item.

Chemical, Biological and Radiological Incidents – be guided by the police.

Responses to CBR incidents will vary more than those involving conventional or incendiary devices, but the following general points should be noted:

- The exact nature of an incident may not be immediately apparent. For example, an Improvised Explosive Device (IED) might also involve the release of CBR material.
- In the event of a suspected CBR incident within a building, switch off all air conditioning, ventilation and other systems or items that circulate air (e.g. fans and personal computers). Do not allow anyone, whether exposed or not, to leave evacuation areas before the emergency services have given medical advice, assessments or treatment.
- If an incident occurs outside an enclosed temporary structure or building, close all doors and windows and switch off any systems that draw air into the building.

Agree your evacuation plan in advance with the police and emergency services, and the local authority. Ensure that staff with particular responsibilities are fully trained, and that

all staff are drilled. Remember, too, to let the police know what action you are taking during any incident.

FM managers should ensure that they have a working knowledge of the heating, ventilation and air conditioning (HVAC) systems and how these may contribute to the spread of CBR materials within the building.

Protected Spaces

Protected spaces in permanent structures may offer the best protection against blast, flying glass and other fragments. They may also offer the best protection when the location of the possible bomb is unknown, when it may be near your external evacuation route.

Since glass and other fragments may kill or maim at a considerable distance from the centre of a large explosion, moving people into protected spaces is often safer than evacuating them onto the streets. Protected spaces should be located:

- In areas surrounded by full - height masonry walls e.g. internal corridors, toilet areas or conference rooms with doors opening inwards.
- Away from windows and external walls.
- Away from the area in between the building's perimeter and the first line of supporting columns (known as the 'perimeter structural bay').
- Away from stairwells or areas with access to lift shafts where these open at ground level onto the street, because blast can travel up them. If, however, the stair and lift cores are entirely enclosed, they could make good protected spaces.
- In an area with enough space to contain the occupants.

When choosing a protected space, seek advice from a structural engineer with knowledge of explosive effects and do not neglect the provision of toilet facilities, seating, drinking water and communications.

Try to locate vital systems in part of your building that offers similar protection to that provided by a protected space.

Communications

Ensure that staff know their roles within the security strategy, and that they or their deputies are always contactable. All staff, including temporary staff, should be familiar with any telephone recording, redial or display facilities and know how to contact police and security staff in or out of office hours.

It is essential to have adequate communications within and between protected spaces. You will at some stage wish to give the 'all clear', or tell staff to remain where they are, to move to another protected space or evacuate the building. Communications may be by public address system (in which case you will need standby power), hand-held radio or other stand alone systems. Do not rely on mobile phones. You also need to communicate with the

emergency services. Whatever systems you choose should be regularly tested and available within the protected space.

Open plan and internal modification

If you have open plan accommodation, remember that the reduction of internal walls reduces protection against blast and fragments.

Interior rooms with reinforced concrete or masonry walls often make suitable protected spaces as they tend to remain intact in the event of an explosion outside the building. If corridors no longer exist, following internal reorganisation for example, then you may also lose your evacuation routes, assembly or protected spaces, while the new layout will probably affect your bomb threat contingency procedures.

When making any such changes, try to ensure that there is no significant reduction in staff protection, for instance by improving glazing protection. If your premises are open plan and there are no suitable protected spaces, then evacuation may be your only option.

Open air events

If you host an event predominantly in the open with only temporary demountable structures such as marquees, or simply an open space, the protected space principle is obviously unlikely to offer any suitable refuge and evacuation may again be your only option.

Explosion – Car Bombs

These can be one of the most effective weapons in the terrorist's arsenal. They are capable of delivering a large quantity of explosives and can cause a great deal of damage. For example, the attack at Glasgow Airport in 2007 carried out by Islamic extremists, and closer to home the Manchester bomb planted by the Provisional IRA in 1996.

Once assembled, the bomb can be delivered at a time of the terrorist's choosing and with reasonable precision. It can be detonated from a safe distance using a timer or remote control, or can be detonated on the spot by a suicide bomber.

Terrorists generally select targets where they can cause most damage, inflict mass casualties or attract widespread publicity.

Effects

Effects are highly destructive. It is not just the effects of a direct bomb blast that can be lethal. Flying debris such as glass can present a hazard many metres away from the seat of the explosion.

What you can do

You may not think your school could be at risk from any form of explosion, however, it is worth remembering one could be deployed locally in a public place nearby, e.g. shops, cinema, town centre etc.

- Insist that details of contract vehicles and the identity of the driver and any passengers approaching your goods/service areas are authorised in advance.
- Establish and rehearse bomb threat and evacuation drills.
- **Train and rehearse your staff in identifying suspect vehicles, and in receiving and acting upon bomb threats. Key information and telephone numbers should be prominently displayed and readily available.**

Chemical, biological and radiological (CBR) attacks

Since the early 1990s, concern that terrorists might use CBR materials as weapons has steadily increased. **The likelihood of a CBR attack remains low, however, it you may have to deal with a hoax call in relation to this or the impact of an attack nearby or in the community**.

Much of the CBR-related activity seen to date has either been criminal, or has **involved hoaxes and false alarms.** CBR weapons have been little used so far, largely due to the difficulty in obtaining the materials and the complexity of using them effectively.

The likelihood of a CBR attack remains low. As with other terrorist attacks, you may not receive prior warning of a CBR incident. Moreover, the exact nature of an incident may not be immediately obvious. First indicators may be the sudden appearance of powders, liquids or strange smells, with or without an immediate effect on people.

Good general physical and personnel security measures already discussed will contribute towards resilience against CBR incidents.

What you can do

- Review the physical security of any air-handling systems, such as access to intakes and outlets.
- Improve air filters or upgrade your air-handling systems, as necessary.
- Restrict access to water tanks and other key utilities.
- **The Home Office advises organisations against the use of CBR detection technologies as part of their contingency planning measures at present. This is because the technology is not yet proven in civil settings and, in the event of a CBR incident the emergency services would come on scene with appropriate detectors and advise accordingly.** A basic awareness of CBR threat and hazards, combined with general protective security measures (e.g. screening visitors, CCTV monitoring and active response of perimeters and entrance areas, being alert to suspicious deliveries) should offer a good level of resilience. In the first instance, seek advice from your local police force CTSA.
- If there is a designated protected space available this may also be suitable as a CBR shelter, but seek specialist advice from your local police force CTSA before you make plans to use it in this way.

- Consider how to communicate necessary safety advice to staff and how to offer reassurance. This needs to include instructions to those who want to leave or return to the site.

Suicide attacks

Although a school may not necessarily seem in to be in this criteria, there are no definitive lists of what would constitute any of the likely targets. Similarly, there is no definitive profile for a suicide bomber, so be aware and remain vigilant.

The use of suicide bombers is a very effective method of delivering an explosive device to a specific location. Suicide bombers may use a lorry, plane or other kind of vehicle as a bomb or may carry or conceal explosives on their persons. Both kinds of attack are generally perpetrated without warning. The most likely targets are mass casualty crowded places, symbolic locations and key installations.

When considering protective measures against suicide bombers, think in terms of:

- Using physical barriers to prevent a hostile vehicle from driving into your site through main entrances, goods/service entrances, pedestrian entrances or open land.
- Denying access to any vehicle that arrives at your goods/service entrances without prior notice and holding vehicles at access control points into your establishment until you can satisfy yourself that they are genuine.
- Wherever possible, establishing your vehicle access control point at a distance from the protected building, briefing staff to look out for anyone behaving suspiciously. Many bomb attacks are preceded by reconnaissance or trial runs. Ensure that such incidents are reported to the police.
- Ensure that no one visits your protected area without your being sure of his or her identity or without proper authority.

Remember there is no definitive physical profile for a suicide bomber, so remain vigilant and report anyone suspicious to the police.

Firearm and weapon attacks

At home in the UK, terrorist use of firearms and weapons is still infrequent but it is important to consider this method of attack and be prepared to cope with such an incident. The attack in Tunisia on British tourists and the attacks on members of the public in Paris are examples of these types of incidents. Please find below some general guidance to aid your planning in this area.

Stay Safe

- Find the best available ballistic protection.
- Remember, out of sight does not necessarily mean out of danger, especially if you are not ballistically protected.

GOOD COVER	BAD COVER
Substantial Brickwork or Concrete	Internal Partition Walls
Engine Blocks	Car Doors
Base of Large Live Trees	Wooden Fences
Natural Ground Undulations	Glazing

See

- Is it a firearms / weapons incident?
- Exact location of the incident.
- Number of gunmen.
- Type of firearm - are they using a long-barrelled weapon or handgun?
- Direction of travel - are they moving in any particular direction?

Consider the use of CCTV and other remote methods of confirming this information, reducing vulnerabilities to staff.

Tell

- **Who** - Immediately contact the police by calling 999, giving them the information shown under **Confirm**
- **How** - use all the channels of communication available to you to inform visitors and staff of the danger.
- *How* you would communicate with staff and visitors?
- What key messages would you give to them in order to keep them safe?
- Think about incorporating this into your emergency planning and briefings

Act

- As far as you can, limit access and secure your immediate environment.
- Encourage people to avoid public areas or access points. If you have rooms at your location, lock the doors if possible and remain quiet.

Further resources on the Stay Safe principles RUN, HIDE, TELL are available from NaCTSO –

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

Hostile reconnaissance

Hostile reconnaissance is the term used to describe the preparatory and operational phases of terrorist operations.

The Primary Role of Reconnaissance by a terrorist

- Obtain a profile of the target location.
- Determine the best method of attack.
- Determine the optimum time to conduct the attack.

They may visit potential targets a number of times prior to the attack. Where pro-active security measures are in place, particular attention is paid to any variations in security patterns and the flow of people in and out.

The ability to recognise those engaged in hostile reconnaissance could disrupt an attack and produce important intelligence leads.

What to look for.
The following sightings or activity may be particularly relevant to your school.

- Significant interest being taken in the outside of your establishment including parking areas, delivery gates, doors and entrances.
- Groups or individuals taking significant interest in the location of CCTV cameras and controlled areas.
- People taking pictures, filming, making notes or sketching of the security measures.
- Overt/covert photography, video cameras, possession of photographs, maps, blueprints etc, of critical infrastructures, electricity transformers, gas pipelines, telephone cables, etc.
- Possession of maps, global positioning systems (GPS), photographic equipment (cameras, zoom lenses, camcorders).
- Vehicles parked outside buildings or other facilities, with one or more people remaining in the vehicle, for longer than would be considered usual.
- Parking, standing or loitering in the same area on numerous occasions with no apparent reasonable explanation.
- Prolonged static surveillance using operatives disguised as demonstrators, street sweepers, etc or stopping and pretending to have car trouble to test response time for emergency services, car recovery companies, (AA, RAC etc) or local staff.
- Simple observation such as staring or quickly looking away.
- Activity inconsistent with the nature of the building.
- Unusual questions - number and routine of staff visiting the school.
- Individuals that look out of place for any reason.

- Individuals that appear to be loitering in public areas.
- Individuals asking questions regarding the identity or characteristics of individual visitors, groups of visitors, or the jobs or nationalities of visitors that may visit the school.
- Persons asking questions regarding security and evacuation measures.
- Persons asking questions regarding staff or student hangouts.
- Persons asking questions regarding VIP visits or events.
- Delivery vehicle in front of the establishment.
- Vehicles, packages, luggage left unattended.
- Vehicles appearing over weight.
- Persons appearing to count pedestrians/vehicles.
- Strangers walking around perimeter of the site.
- Persons loitering around area for a prolonged amount of time.
- Persons attempting to access plant equipment or chemical areas.
- Delivery vehicles or other trucks attempting to access the main driveway to the school.
- Delivery vehicles arriving at the school at the wrong time or outside of normal hours.
- Vehicles emitting suspicious odours e.g. fuel or gas.
- Vehicle looking out of place.
- Erratic driving.
- Questions regarding the school structure.
- Noted pattern or series of false alarms indicating possible testing of security systems and observation of response behaviour and procedures, (bomb threats, leaving hoax devices or packages).
- The same vehicle and different individuals or the same individuals in a different vehicle returning to a location.
- The same or similar individuals returning to carry out the same activity.
- Unusual activity by contractor's vehicles.
- Recent damage to perimeter security, breaches in fence lines or walls or the concealment in hiding places of equipment, i.e. ropes, ladders, food etc. Regular perimeter patrols should be instigated months in advance of a high profile event to ensure this is not happening.
- Attempts to disguise identity - motorcycle helmets, hoodies, etc. or multiple sets of clothing to change appearance.
- Constant use of different paths, and/or access routes across a site. 'Learning the route' or foot surveillance involving a number of people who seem individual but are working together.

- Multiple identification documents - suspicious, counterfeit, altered documents etc.
- Non co-operation with police or security/site personnel.
- Those engaged in reconnaissance will often attempt to enter premises to assess the internal layout and in doing so will alter their appearance and provide cover stories.
- In the past reconnaissance operatives have drawn attention to themselves by asking peculiar and in depth questions of employees or others more familiar with the environment.
- Sightings of suspicious activity should be passed immediately to management for CCTV monitoring, active response where possible and the event recorded for evidential purposes.

THE ROLE OF RECONNAISSANCE HAS BECOME INCREASINGLY IMPORTANT TO TERRORIST OPERATIONS.

Reconnaissance trips may be undertaken as a rehearsal to involve personnel and equipment that will be used in the actual attack e.g. before the London attacks on 7th July 2005, the bombers staged a trial run nine days before the actual attack.

Reporting suspicious activity to police that does not require an immediate response, contact the CONFIDENTIAL ANTI-TERRORIST HOTLINE - 0800 789 321

ANY INCIDENT THAT REQUIRES AN IMMEDIATE RESPONSE - DIAL 999.

Contact the local authority education security specialist for access to the **DVD 'Operation Fairway'** for use in any training sessions.

Events

Although schools do not necessarily host high profile events very often, there may be times when events are held at your school, which for various reasons, are deemed to be more high profile and therefore more vulnerable to attack e.g. Opening Ceremonies attended by Members of Parliament or Royalty etc. This may involve pre-event publicity of the attendance of a VIP or celebrity, resulting in additional crowd density on the event day and the need for an appropriate security response and increased vigilance.

Enhanced Security Provision at High Profile Events

During High Profile Events there may be extra threats not only from terrorism but criminal activity, politically disruptive groups, fixated persons, self-publicists and lone adventurers.

Dependent on the nature of the threat and outcome of the risk management process, consideration should be given to a range of physical, technical and procedural protective security options that may, on their own, be sufficient to exclude, deter, detect or disrupt the threat.

What measures to consider

Physical and technical security measures may include:

- Physical protection measures such as extra doors, locks and lighting.
- Technical measures including enhanced or extended CCTV and alarms if required.
- Vehicle security at the event site such as marshalling, security patrols etc.
- Early identification of all organisations involved in the event, their roles and responsibilities.
- The circumstances under which an event will be discontinued and the method and ownership for such decisions, and means by which by which this will be communicated.
- The circumstances under which a venue will be evacuated and VIP's removed.
- Clarification of the role, powers and capability of any private security staff or stewards either permanent or temporarily contracted for the specific event.
- Prepare lists for restricted circulation only to partners (see care and retention of sensitive material above), incorporating invited and confirmed guests, chronology of events, copies of invitations, car passes and any other relevant materials, such as plans, maps and contact lists, etc.
- Specimen copies of any accreditation passes and badges allowing access to the various zones, etc.
- Create security zones within the secure perimeter to segregate VIP's from invited guests, the general public and the media, etc. Consider providing a 'Green Room' or place of safety where a VIP could shelter in the event of an incident.

- Identity safe routes to and from the venue, as well as safe evacuation / escape routes.
- Arrangement of parking for VIP vehicles and introduction of parking restrictions locally if a bomb threat is identified.

Threat levels

Information about the national threat level is available on the MI5 - Security Service website.

Terrorism threat levels are designed to give a broad indication of the likelihood of a terrorist attack. They are based on the assessment of a range of factors including current intelligence, recent events and what is known about terrorist intentions and capabilities. This information may well be incomplete and decisions about the appropriate security response should be made with this in mind.

Threat Level Definitions

CRITICAL	AN ATTACK IS EXPECTED IMMINENTLY
SEVERE	AN ATTACK IS HIGHLY LIKELY
SUBSTANTIAL	AN ATTACK IS A STRONG POSSIBILITY
MODERATE	AN ATTACK IS POSSIBLE BUT NOT LIKELY
LOW	AN ATTACK IS UNLIKELY

Response Levels

Response levels provide a broad indication of the protective security measures that should be applied at any particular time. They are informed by the threat level but also take into account specific assessments of vulnerability and risk.

Response levels tend to relate to sites, whereas threat levels usually relate to broad areas of activity.

There are a variety of site specific security measures that can be applied within response levels, although the same measures will not be found at every location.

The security measures deployed at different response levels should not be made public, to avoid informing terrorists about what we know and what we are doing about it.

There are three levels of response which broadly equate to threat levels as shown below:

CRITICAL	EXCEPTIONAL
SEVERE	HEIGHTENED
SUBSTANTIAL	
MODERATE	NORMAL
LOW	

Response Level Definitions

RESPONSE LEVEL	DESCRIPTION
EXCEPTIONAL	Maximum protective security measures to meet specific threats and to minimise vulnerability and risk.
HEIGHTENED	Additional and sustainable protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk.
NORMAL	Routine baseline protective security measures, appropriate to your business and location.

Communication and training

You should consider a communication strategy or staff vigilance campaign for raising awareness among staff and others who need to know about your security plan and its operation.

The consideration of a signage strategy incorporating placement, size and directional activity is a key aspect of an overall communication strategy. The delivery of effective and efficient movement possibilities from one area to another reduces tensions during an evacuation, invacuation or other threat situation.

There should also be arrangements for dealing with people who may be affected by your security operation but who are not employees of your organisation (e.g. pupils, parents contractors, visitors).

It should be remembered that immediately following a terrorist attack, mobile telephone communication may be unavailable due to excessive demand, so consideration should be given to alternative communication.

Consideration should be given to the use of any website and/or publications that could communicate crime prevention and counter terrorism initiatives.

Further training or presentations such as Project Argus or Operation Fairway (DVD) may be available for suitable staff via your local Education Security Specialist or Counter Terrorism Security Advisor. Contact deborah.borg@salford.gov.uk for further information.

Grab bag checklist

Items you could consider including in a grab bag sometimes known as a battle or incident box.

Equipment:

- Emergency and Floor plans (laminated)
- List of Contacts staff etc (laminated)
- Incident Log, notebook, pens, markers, etc
- First aid kit (designed for major emergencies) consider large bandages, burn shields or cling film, large sterile strips, cold packs, baby wipes as well as standard equipment
- Torch and spare batteries or wind up
- High visibility jackets
- Foil blankets / bin liners
- Water and chocolate/glucose tablets
- Mobile telephone with credit available, plus charger

Documents should be electronically stored and accessible remotely, otherwise paper copy should be readily available:

- Business Continuity Plan
- Communication strategy, signage and messaging
- List of employees with contact details - include home and mobile numbers. You may also wish to include next-of-kin contact details.
- Contact details for utility companies that supply your gas/electric/water.
- Building site plan, including location of gas, electricity and water shut off points.
- Insurance company details.
- Local Authority Emergency Liaison contact details

Make sure the pack is stored safely and securely site on site or at an accessible emergency location nearby. Remember that cash / credit cards may be needed for emergency expenditure.

This list is not exhaustive, and there may be other documents or equipment that should be included for your school. You know the organisation best.

Bomb threat checklist

This checklist is designed to help your staff to deal with a telephoned bomb threat effectively and to record the necessary information on this sheet.

Actions to be taken on receipt of a bomb threat:

1. Tell the caller which town/district you are answering from.
2. Record the exact wording of the threat:

Ask the following questions:

Where is the bomb right now?

When is it going to explode?

What does it look like?

What kind of bomb is it?

What will cause it to explode?

Did you place the bomb?

Why?

What is your name?

What is your address?

What is your telephone number?

(Record time call completed:)

Where automatic number reveal equipment is available, record number shown:

Inform the premises manager of name and telephone number of the person informed:

Contact the police on 999. Time informed:

The following part should be completed once the caller has hung up and the premises manager has been informed.

Time and date of call:

Length of call:

Number at which call was received (i.e. your extension number):

ABOUT THE CALLER

Sex of caller:

Nationality:

Age:

THREAT LANGUAGE (tick)

❒ Well spoken?
❒ Irrational?
❒ Taped message?
❒ Offensive?
❒ Incoherent?
❒ Message read by threat-maker?

CALLER'S VOICE (tick)

❒ Calm?
❒ Crying?
❒ Clearing throat?
❒ Angry?
❒ Nasal?
❒ Slurred?
❒ Excited?

❒ Stutter?
❒ Disguised?
❒ Slow?
❒ Lisp?
❒ Accent? If so, what type?_____
❒ Rapid?
❒ Deep?
❒ Hoarse?
❒ Laughter?
❒ Familiar? If so, whose voice did it sound like? _____

BACKGROUND SOUNDS (tick)

❒ Street noises?
❒ House noises?
❒ Animal noises?
❒ Crockery?
❒ Motor?
❒ Clear?
❒ Voice?
❒ Static?
❒ PA system?
❒ Booth?
❒ Music?
❒ Factory machinery?
❒ Office machinery?
❒ Other? (specify) _____

OTHER REMARKS

_____
_____
_____
_____

Signature

_____

Date _____

Print name

_____