101 – Police non-emergency number 999 – Police emergency number
0800 789 321 – Confidential Anti-Terrorist Hotline

EVENT ORGANISER's SECURITY ADVICE;
Avon & Somerset POLICE
Counter-Terrorism Security Coordinator

We are grateful that you are taking the time to read this guidance and advice document. Bringing Security into your thoughts for your organisation and event is essential so that you can plan for a safe and secure event in advance. Later in the document we will provide links to other more detailed sources of information. This document is aimed to give you an overview and allow you to then research further around specific areas if required.

There is no intelligence to suggest that your event is any more at risk than any other, however it remains a possibility, however small that someone may wish to carry out a hostile act using your event as a platform. Terrorism in many forms and as a threat, sadly remains at the forefront of our thinking when planning for events. So thank you for refreshing your awareness.

UK Government support raising the awareness around considering hostile threats through their ACT programme (Action Counters Terrorism), which includes access to on-line training. We encourage you to access as an aid to you, your colleagues, your event and your organisation.

https://www.gov.uk/government/news/act-awareness-elearning

Of note a useful phone app called 'URIM' which give further access to information.

Apple App Store - https://apps.apple.com/gb/app/urim/id1310305478

Google Play
App Store - https://play.google.com/store/apps/details?id=com.app.urim

Security Plans for your event;

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 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 and in-vacuation plans and details on securing the attraction in the event of a major incident
- Your business continuity plan
- A communications and media strategy which includes handling enquiries from concerned family and friends.

Hostile Reconnaissance

Terrorists very often undertake some form of reconnaissance before carrying out an attack. They may do this in vehicles or on foot, recording and documenting locations.

In periods of heightened alert, it is vital to remain vigilant, trust your instincts and report possible reconnaissance to the police.

What to look for

- Significant interest being taken in the outside of your event site 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 around events. Tourists should not necessarily be taken as such and should be treated sensitively, but with caution.
- 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). GPS will assist in the positioning and correct guidance of weapons such as mortars and Rocket Propelled Grenades (RPGs). This should be considered a possibility up to one kilometre from any target.
- Vehicles parked outside buildings of 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 or event.

- Unusual questions - number and routine of staff/VIP's visiting the site or event.
- 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 attend or may visit the event.
- Persons asking questions regarding security and evacuation measures.
- Persons asking questions regarding event staff hangouts.
- Persons asking questions regarding VIP visits.
- Delivery vehicle in front of the event.
- Vehicles, packages, luggage left unattended.
- Vehicles appearing over weight.
- Persons appearing to count pedestrians/vehicles.
- Strangers walking around perimeter of the event.
- People 'nursing' drinks and being over attentive to surroundings. 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 event.
- Delivery vehicles arriving at the event 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 event 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(s).
- The same or similar individuals returning to carry out the same activity to establish the optimum time to conduct the operation.
- Unusual activity by contractor's vehicles.
- Recent damage to perimeter security, breaches in fence lines or walls or the concealment in hides of mortar base plates or assault 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 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 security management for CCTV monitoring, active response where possible and the event recorded for evidential purposes.
- Vehicles moving slowly near public buildings, structures or bridges, or parked in suspicious circumstances
- People using recording equipment, including camera phones or seen making notes or sketches for no apparent reason – especially of staff or security features
- Attention to specific access/egress areas, stairwells, hallways and fire escapes for no apparent reason
- Deliveries to venue - questions to ask could include, is the delivery from a known supplier and is it expected? Is there anything unusual about the packaging or item?
- Members of the public in offices and ‘off limits’ areas, plant rooms and similar locations
- Someone taking an interest in staff/vehicle movements
- Inappropriate approaches to any staff member
- Someone being followed
- Packages/bags being left unattended
- Anything you feel isn’t right

Good Housekeeping

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

Encourage Staff/ Volunteers to undertake the following;

- Be extra vigilant

- Report any suspicious behaviour / incidents in the lead up to the event and on the day
- Challenge anyone not recognised in areas out of bounds to the public
- Report any alarm activations at relevant buildings
- You CAN approach a person that has been seen acting in a suspicious manner and ask them to account for their actions.
- You CANNOT stop or detain that person or prevent them from leaving if they decline to answer.
- NO power exists in law to prevent a person from taking a photograph of anything or any person in a public place.
- NO power exists in law to require that any images taken be deleted.
- Security personnel do NOT have powers to ask to view images.
- Security personnel do NOT have powers to seize equipment used to take an image.
- Powers under S.43 Terrorism Act 2000 to stop, examine and seize are ONLY available to Police Officers who should be called if required.

Search

PAS-127 is the accepted standard applied to search regimes. Search locations must be positioned in an appropriate location and have regard to the welfare of security staff being sheltered from the elements so that they maintain a focus. 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.

Searches may be used as part of routine good housekeeping. Staff should be looking for anything;

- that should not be there
- that cannot be accounted for
- that is out of place

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, business 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.

Suspicious Items/packages – The HOT PRINCIPLES

Consider using the below when dealing with an unattended bag or item when there is no other information or intelligence to suggest that it is suspicious;

H – Hidden

- Hidden deliberately? Has a deliberate attempt been made to hide item

O – Obvious

- Obviously suspicious? / Why has it been abandoned

T – Typical

- Typical of what you would expect to find at location
- Lots of the crowd will have bags

If upon finding an item and having gone through the HOT principles you believe it is suspicious then follow the 4 C's:

- **CONFIRM** – Confirm that YOU believe the item to be suspicious
- **CLEAR** – Clear the area and cordon if possible
- **COMMUNICATE** – Call 999, communicate internally, and do not use phones or mobiles within 15 metres.
- **CONTROL** – Control cordon and scene

INFORMATION TO PASS TO THE POLICE

WHAT is it? – Size, component

WHERE is it? – Location, access routes

WHEN was it left? When was it found? – Has it been moved?

WHY is it suspicious?

WHO – Were there any suspects? Are there any witnesses?

Suspicious Behaviour

Organisations and events face a variety of threats: terrorists, activists and criminals. While these threats and their aims may vary, hostiles are united in their desire to succeed. Recognising they may not get a second chance to achieve their aims, hostiles will typically plan carefully. They may do this on foot or in vehicles, alone or in a group and maybe seen to document their findings either by making notes or taking photographs or video.

It is essential that you report incidents of suspicious behaviour to the police and to the Organisers; and where feasible challenge it.

- You CAN approach a person that has been seen acting in a suspicious manner and ask them to account for their actions.
- You CANNOT stop or detain that person or prevent them from leaving if they decline to answer.
- NO power exists in law to prevent a person from taking a photograph of anything or any person in a public place.
- NO power exists in law to require that any images taken be deleted.
- Security personnel do NOT have powers to ask to view images.
- Security personnel do NOT have powers to seize equipment used to take an image.

Powers under S.43 Terrorism Act 2000 to stop, examine and seize are ONLY available to Police Officers who should be called if required.

Delivered items

Letters, parcels, packages and other items delivered by post or courier have been used on occasions to disguise harmful devices and substances. Delivered items may be explosive, incendiary, sharps or blades, or conceivably contain chemical, biological or radiological material. Other hazardous or offensive material such as faeces, have also been used in delivered items.

Anyone receiving a suspicious delivery is unlikely to know what type it is, so procedures and precautions should cater for every eventuality. A delivered item will probably have received fairly rough handling in the post, so is unlikely to detonate because it is moved. Any attempt to open such an item may well set it off. Threat items come in a wide range of shapes and sizes. A well-made device will look innocuous but may still have tell-tale signs.

- Unexpected item, especially if hand delivered.
- A padded envelope or other bulky package.
- An additional inner envelope or other contents that may be difficult to remove.
- Labelling or excessive sealing that encourages opening at a particular end or in a specific way.
- Oddly-shaped or lop-sided.
- Envelope flap completely stuck down.
- Marked ‘To be opened by’, ‘Personal’ or ‘Confidential’.
- Item addressed to the organisation or a job title rather than a named person.
- Item addressed to a high profile individual.
- Unexpected or unusual origin (postmark and/or return address).
- Poorly or inaccurately addressed.
- Address printed unusually or unevenly e.g. using a lettering stencil.
- Unfamiliar style of writing.
- No return address or a return address that cannot be verified.
- Unusual postmarks or no postmarks.
- More stamps than needed for the size and weight of the package.
- Unusual smell.
- Greasy or oily stains emerging from within.
- Small hole(s) in the envelope or wrapping.
- Powders or liquids emanating from the package.
- Sudden onset of illness or irritation of skin, eyes or nose.

If in doubt call 999 and ask for the police. Clear the area immediately. Do not attempt to open the letter or package. Avoid unnecessary handling. Keep it separate so it is easily identifiable.

Telephone threats and anonymous calls

Anonymous calls and telephone threats are usually intended to lower your morale or cause fear, alarm and distress. These calls can be extremely distressing but, if it is bearable, keeping the caller talking can reveal important information. If the call is not too upsetting, consider the following actions:

- Note details about the caller: e.g. gender, accent, a speech impediment.

- Listen for any clues as to the intention of the caller or the specific threat.
- Listen for background noise, which may provide valuable information about the location or circumstances of the caller (traffic, trains, children etc.).
- Write down the details immediately; include date, time and exact words spoken, if possible.
- Keep a note pad and pen to hand.
- On termination of the call operate any trace facility, such as the BT 1471 service.
- Inform the police immediately if threats have been made.
- Consider making your home phone number ex-directory.

Vehicle Borne Improvised Explosive Device

Vehicle Borne Improvised Explosive Devices (VBIEDs) are one of the most effective weapons in the terrorist's arsenal. They are capable of delivering a large quantity of explosives to a target and can cause a great deal of damage.
What you can do;

If you think your event could be at risk from any form of VBIED you should:

- Ensure you have effective vehicle access controls, particularly at goods entrances and service yards. Do not allow unchecked vehicles to park within the event areas or next to public areas where there will be large numbers of people or where there is a risk of structural collapse.
- Denying access to any vehicle that arrives at your goods/service entrances without prior notice and holding vehicles at access control points into your event until you can satisfy yourself that they are genuine.
- Wherever possible, establishing your vehicle access control point at a distance from the protected site, setting up regular patrols and briefing staff to look out for anyone behaving suspiciously.
- Insist that details of contract vehicles and the identity of the driver and any passengers approaching your goods/service areas are authorised in advance.
- Consider a vehicle search regime at goods/service entrances that is flexible and can be tailored to a change in threat or response level. It may be necessary to carry out a risk assessment for the benefit of security staff who may be involved in vehicle access control.
- Establish and rehearse bomb threat and evacuation drills. Bear in mind that, depending on where the suspected VBIED is parked and the layout of your event, it may be safer in windowless corridors or basements than outside if this facility is available.
- Consider using robust physical barriers to keep all but authorised vehicles at a safe distance.

- 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.

101 – Police non-emergency number 999 – Police emergency number
0800 789 321 – Confidential Anti-Terrorist Hotline

Weapons / Firearms attacks

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. Below is some general guidance to aid your planning in this area.

Stay Safe

IN THE RARE EVENT OF a firearms or weapons attack - RUN HIDE TELL

RUN to a place of safety. This is a far better option than to surrender or negotiate. If there's nowhere to go, then…

HIDE It's better to hide than to confront. Remember to turn your phone to silent and turn off vibrate. Barricade yourself in if you can. Then finally and only when it is safe to do so…

TELL the police by calling 999.

- 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

- It is 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 confirmation reducing vulnerabilities to staff.

Plan - for a firearms / weapons incident

- 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 your have rooms at your location, lock the doors if possible and remain quiet.

Chemical Biological Radiological

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 will contribute towards resilience against CBR incidents. Remember to apply appropriate personnel security standards to contractors, especially those with frequent access to your site.

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.
- Review the security of your food and drink supply chains.

Remove, Remove, Remove.

If you think someone has been exposed to a HAZARDOUS SUBSTANCE

Use caution and keep a safe distance to avoid exposure yourself. ACT QUICKLY.

These actions can SAVE LIVES.

TELL THOSE AFFECTED TO:

REMOVE THEM...from the immediate area to avoid further exposure to the substance. Fresh air is important. If the skin is itchy or painful, find a water source.

101 – Police non-emergency number 999 – Police emergency number
0800 789 321 – Confidential Anti-Terrorist Hotline

REPORT...Dial 999

REMOVE OUTER CLOTHING...If affected by the substance.

Try to avoid pulling clothing over the head if possible. Do not smoke, eat or drink. Do not pull off clothing stuck to skin.

REMOVE THE SUBSTANCE... from skin using a dry absorbent material to either soak it up or brush it off.

RINSE continually with water if the skin is itchy or painful.

REMEMBER:

Exposure is not always obvious. SIGNS CAN INCLUDE:

- The presence of hazardous or unusual materials.
- A change in environment, such as unexplained vapour, odd smells or tastes.
- Unexplained signs of skin, eye or airway irritation, nausea, vomiting, twitching, sweating, disorientation, breathing difficulties.

DRONES – UNMANNED AERIAL VEHICLES (UAV's)

Whether intentional or not, the disruptive effect a drone can cause is notable. If you see a drone being flown at the site and are concerned it may cause a hazard, under normal circumstances try and speak with the operator.

- Be professional and polite and ask them questions, someone might be recording your actions. Record all of the details. Remember they are under no obligation to provide you with any information.
- Full details of the incident should be recorded whether the suspect has confirmed his/her identity or not.
- You should not attempt to remove the controller or the drone without permission of its owner.

If you suspect suspicious activity, dial 999 for a police officer's assistance and report to the Organisers Office. Police officers have additional powers to deal with such an incident.

Information Security

The loss of confidentiality, integrity and most importantly availability of information in paper or digital format can be a critical problem for organisations. Many rely on their information systems to carry out business or nationally critical functions and manage safety and engineering systems.

Your confidential information may be of interest to business competitors, criminals, foreign intelligence services or terrorists. They may attempt to access your information by breaking into your IT systems, by obtaining the data you have thrown away or by infiltrating your organisation. Such an attack could disrupt your business and damage your reputation.

When considering this type of attack you should look at facilities and processes at your event site and any other place you operate from. Many large event organisers will contract in security access control systems. Make sure it is clear who is responsible for management and security of data.

What can you do

- Acquire your IT systems from reputable manufacturers and suppliers.
- Ensure that your software is regularly updated. Suppliers are continually fixing security vulnerabilities in their software. These fixes or patches are available from their websites - consider checking for patches and updates daily.
- Ensure that all internet-connected computers are equipped with anti-virus software and are protected by a firewall.
- Back up your information, preferably keeping a secure copy in another location.
- Assess the reliability of those who maintain, operate and guard your systems
- Consider encryption packages for material you want to protect, particularly if taken offsite - but seek expert advice first.
- Take basic security precautions to prevent software or other sensitive information falling into the wrong hands. Encourage security awareness among your staff, training them not to leave sensitive material lying around and to operate a clear desk policy (i.e. desks to be cleared of all work material at the end of each working session).
- Make sure your staff are aware that users can be tricked into revealing information which can be used to gain access to a system, such as user names and passwords.
- Invest in secure cabinets, fit locking doors and ensure the proper destruction of sensitive material

- Where possible, lock down or disable disk drives, USB ports and wireless connections.
- Ensure computer access is protected by securely controlled, individual passwords or by biometrics and passwords.
- Implement an acceptable use policy for staff concerning web browsing, email, use of chat rooms, social sites, trading, games and music download websites.

An Incident

In the event of an incident at your event – reporting information to the Emergency Services using the METHANE pneumonic is useful to ensure the correct response is made.

Accurate initial information gathering will result in a faster and more accurate response for the general public from the emergency services

- Major Incident declared?
- Exact Location
- Type of incident
- Hazards present or suspected
- Access – routes that are safe to use
- Number, type, severity of casualties
- Emergency services present and those required

101 – Police non-emergency number 999 – Police emergency number
0800 789 321 – Confidential Anti-Terrorist Hotline

STAY SAFE

In the rare event of a Firearms or weapons attack

REMEMBER

RUN



Run to a place of safety. This is a far better option than to surrender or negotiate. If there's nowhere to go, then…

HIDE



It's better to hide than to confront. Remember to turn your phone to silent and turn off vibrate. Barricade yourself in if you can. Then finally and only when it is safe to do so…

TELL



Tell the police by calling 999.

So stay safe, and just remember the words: RUN. HIDE. TELL.

Further and more detailed security advice is available to you at

www.gov.uk/ACT

https://www.cpni.gov.uk/advice-guidance

https://www.counterterrorism.police.uk/

Additionally please do not hesitate to contact the CT Security Coordinator or Police Operational or Event Planner associated with your event if you have any further enquiries.

Avon & Somerset Constabulary
CT Security Co-ordinators 2021

Avon and Somerset Police
SERVE.PROTECT.RESPECT.
www.avonandsomerset.police.uk | Follow us on