



Incident Response Playbook

Table of Contents

.....	1
Purpose and Context.....	6
Scope of the Playbook.....	6
How to Use the Playbook.....	7
Practical Application for Responsible Persons	8
Multi-Agency Collaboration.....	9
Stakeholder groups and support.....	10
Decision-Making Under Pressure.....	10
A. Suspicious Items	11
Key Considerations	11
Resources	11
Identifying a Suspicious Item	11
Immediate Actions	11
Notify Authorities	12
Communicate with Staff and Attendees	12
Post-Incident Actions	12
B. Improvised Explosive Device (IED) Scenario.....	12
Recognising an IED Threat	13
Key Considerations	13
Immediate Actions	13
Communication Advice for Mobile Phones and Radios.....	14
Communication Protocols	14
Post-Incident Actions	15
Preventative Measures	15
Supporting Tools.....	16
C. Hostile Reconnaissance	16
Key Considerations	16
Resources	16
Preventative Measures	16
Recognising Hostile Reconnaissance	17
Immediate Actions	18
Escalation Process.....	18
Communication Protocols	18
Post-Incident Actions	18
D. Marauding Attacker - Knife / Gunman	19
Key Considerations	19
Resources	19
Preventative Measures	19
Recognising the Threat	19
Immediate Actions	20
Communication Protocols	20
Role-Specific Actions	20
Post-Incident Actions	21
E. Crowd Management Issues.....	21
Recognising Crowd Management Issues	21

Preventative Measures	22
Immediate Actions	22
Communication Protocols	22
Post-Incident Actions	22
F. Mass Casualty Event	23
Recognising a Mass Casualty Event	23
Preventative Measures	23
Immediate Actions	23
Communication Protocols	23
Post-Incident Actions	23
G. Adverse or Severe Weather	24
Recognising Adverse or Severe Weather Risks	24
Preventative Measures	24
Key Weather Conditions to Monitor	24
Action Levels and Corresponding Responses	25
Immediate Actions	27
Communication Protocols	27
Post-Incident Actions	28
Supporting Tools	28
H. Hazardous Materials (HAZMAT)	28
Recognising a HAZMAT Incident	28
Immediate Questions to Assess the Situation:	28
Key Considerations	29
Preventative Measures	29
Immediate Actions	29
If you have been affected:	30
Communication Protocols	31
Post-Incident Actions	31
Supporting Tools	32
Some other responses you may wish to consider:	32
I. Lost or Missing Person (See also DSC Lost or Vulnerable Persons Procedures)	32
Recognising a Lost or Missing Person Situation	32
Immediate Actions	32
Communication Protocols	33
Post-Incident Actions	33
Preventative Measures	34
J. Vulnerable Person Assistance	34
Immediate Actions	34
Communication Protocols	35
Post-Incident Actions	35
Preventative Measures	35
K. Cybersecurity Breach or Digital Disruption	36
Recognising a Cybersecurity Breach or Digital Disruption	36
Immediate Actions	36
Communication Protocols	36
Post-Incident Actions	37
L. Fire or Smoke Detection	37
Recognising a Fire or Smoke Incident	37
Immediate Actions	37
Communication Protocols	38

Post-Incident Actions	38
M. Power Outage or Technical Failure	38
Recognising a Power Outage or Technical Failure	38
Immediate Actions	39
Communication Protocols	39
Post-Incident Actions	39
N. Dangerous Animal or Wildlife Intrusion	40
Recognising a Dangerous Animal or Wildlife Intrusion	40
Immediate Actions	40
Communication Protocols	40
Post-Incident Actions	40
O. Handling Media and Press Attention	41
Key Benefits of Effective Media Handling	41
When to Engage with the Media	41
Principles for Media Engagement	41
Designating a Spokesperson	42
Key Considerations Before Speaking to the Media	42
Avoiding Common Pitfalls.....	42
Post-Media Engagement Actions	43
Dealing with Intrusive Media Attention.....	43
Strategies for Managing Intrusive Media.....	43
Example Scripts for Challenging Scenarios	44
Escalation Protocols	44
Preventative Measures	45
Benefits of Managing Intrusive Media Effectively	45
Media and Press Interaction Cheat Sheet	45
<i>Scripts for responding to Common Scenarios</i>	46
Key Tips for Handling Interviews:	47
General Principles for All Interviews	47
P. Media Interview Cheat Sheets	48
1. Face-to-Face Interviews	48
2. Piece to Camera	48
3. Phone Interviews	49
4. Down-the-Line Interviews.....	49
5. Closing the Interview	49
6. Final Do's and Don'ts	50
Q. Joint Emergency Services Interoperability Principles (JESIP)	50
1. What is JESIP?	50
2. The Five JESIP Principles	50
3. The M/ETHANE Model.....	51
4. Why JESIP Matters for Venues and Events:	52
5. Actions for Event Organisers	52
R. Incident Reporting Template	52
S. Staff Briefing Checklist	53
T. Suspicious Item Reporting Form	55
U. Draft Information Sharing Agreement (ISA) Template	56
The legal bit: Decision Support Centre (DSC) & National Events Database (NED)	
Disclaimers	60
1. General Disclaimer	60

2. Limitation of Liability	61
3. No Guarantee of Outcomes	61
4. User Responsibility	61
5. Third-Party Links or References.....	61
6. Intellectual Property Disclaimer	61
7. Compliance with Regulations	62
8. Tailored Solutions Disclaimer	62



Purpose and Context

The Decision Support Centre (DSC) Incident Response Playbook provides practical guidance to support venues, events and organisations in recognising, responding to and recovering from a wide range of safety and security incidents.

The Playbook does not assume that specific threats can be predicted. It is designed to support structured response to a range of possible scenarios.

It is designed to support how decisions are made in real-world environments - where information may be incomplete, situations evolve rapidly, and multiple teams and partners are required to act in a coordinated way.

While informed by the intent of the Terrorism (Protection of Premises) Act 2025 (Martyn's Law), the Playbook is not limited to legislative requirements. It focuses on applying proportionate, practical actions that protect people and support effective operational outcomes.

At its core, the Playbook supports a structured approach:

Recognise → Assess → Decide → Act → Review

This approach reflects the reality that effective incident response depends not only on having plans, but on how individuals and teams interpret information, communicate and act under pressure.

This also reflects the reality that decisions are often made with incomplete or evolving information.

The Playbook is intended to be used alongside the DSC Events & Venues Toolkit and Responsible Persons Training, forming part of a wider approach to preparedness, readiness and organisational resilience.

Scope of the Playbook

The Playbook is structured around high-risk, high-impact scenarios commonly encountered in venues and events, providing practical guidance that can be adapted to different environments and scales.

Each scenario includes:

- recognition indicators
- key considerations
- immediate actions
- communication approaches

- escalation and coordination
- post-incident review and recovery

These scenarios are not intended to be followed rigidly. They provide a framework to support informed decision-making, recognising that no two incidents will unfold in exactly the same way.

The Playbook supports the full operational lifecycle:

- Business as Usual (BAU) awareness and early identification
- Escalation and response
- Stabilisation and coordination with partners
- Recovery and return to normal operations

It is designed to complement existing plans, procedures and local arrangements, not replace them.

Actions should be proportionate to the nature and scale of the incident and adapted to the specific environment.

Topics include:

- Suspicious Items
- Improvised Explosive Devices (IEDs)
- Hostile Reconnaissance
- Marauding Attacks (Knife/Gun)
- Crowd Management Issues
- Mass Casualty Events
- Adverse or Severe Weather
- Hazardous Materials (HAZMAT)
- Lost or Missing Persons
- Vulnerable Persons Assistance
- Cybersecurity Breaches or Digital Disruption
- Fire or Smoke Detection
- Power Outages or Technical Failure
- Dangerous Animal or Wildlife Intrusion
- Handling Media and Press Attention
- Media Interview Cheat Sheets
- Joint Emergency Services Interoperability Principles (JESIP)
- Incident Reporting Template
- Staff Briefing Template
- Suspicious Item Reporting Form

How to Use the Playbook

The Playbook is intended to be used as a working resource before, during and after incidents.

It can support:

- **Planning and preparation** - informing procedures, briefings and risk assessments
- **Training and validation** - through tabletop exercises, walkthroughs and simulations
- **Live incident response** - as a reference point for structured action and communication
- **Recovery** - to assist with the recovery and the safe return to normal operations
- **Post-incident review** - supporting learning and continuous improvement

It should be integrated with:

- the DSC Events & Venues Toolkit
- organisational plans and procedures
- local authority and emergency service arrangements

The Playbook is most effective when used as part of a wider approach to readiness, where:

- roles and responsibilities are understood
- communication pathways are clear
- and teams have confidence in applying guidance in practice

What this Playbook Is designed to do:

- Support structured response
- Improve coordination
- Build confidence in decision-making

What it is not:

- A rigid set of instructions
- A substitute for judgement
- A complete solution for every scenario

Practical Application for Responsible Persons

The Playbook supports the Responsible Person in fulfilling their role by providing a structured approach to incident response that can be applied across different scenarios.

The Responsible Person is not expected to control every aspect of an incident. Their role is to:

- maintain oversight
- support coordination
- ensure decisions are informed and proportionate
- and facilitate effective communication between teams and partners

In practice, this means working across three interconnected areas:

- Responsibility - accountability for outcomes
- Control - where operational decision-making sits
- Influence - the wider environment, including partners, agencies and external factors

The Playbook supports this by helping Responsible Persons:

- understand how incidents develop
- recognise when to escalate
- coordinate with others effectively
- and support a transition from response into recovery

Benefits to Venues and Events:

- Strengthens preparedness and operational resilience
- Supports structured, confident decision-making under pressure
- Enhances coordination across teams and partner organisations
- Builds staff confidence through clear, practical guidance
- Supports consistent approaches to response and recovery

Multi-Agency Collaboration

- **Integration with Local Authorities:**
 - Ensure your own playbooks align with local Safety Advisory Group (SAG) recommendations (see the DSC Toolkit for more information on SAG participation)
 - Include contacts and escalation paths for rapid coordination
- **Mutual Aid Agreements:**
 - Establish protocols for seeking assistance from nearby venues or organisations during large-scale emergencies
 - Information Sharing Agreement(s) to support multi-agency collaboration ([see section U. DSC Information Sharing Agreement](#))

Stakeholder groups and support

- **Establish links with land and venue owners:**
 - Ensure your own playbooks align with local Safety Advisory Group (SAG) advice.
- **Identify local resources:**
 - Map out the location of and routes to local medical facilities and hospitals particularly those with A&E
 - Compile a list of back-up resources such as potable and bottled water, generators, fuel, ponchos etc.

Decision-Making Under Pressure

During incidents, information may be incomplete, conflicting or rapidly changing.

The aim is not to achieve perfect information, but to make informed, proportionate decisions based on what is known at the time.

The following principles apply:

- act on credible information, not assumption
- prioritise life safety and clear communication
- escalate early where appropriate
- adapt as new information becomes available

Following each scenario or incident, ensure actions, decisions and observations are recorded and reviewed to support learning and future preparedness.

Try to maintain a calm, controlled response to support clear communication and decision-making.

This resource forms part of a wider DSC ecosystem, including:

- Events & Venues Toolkit
- DSC's Responsible Persons Training
- National Events Database (NED)

Together, these provide a coordinated approach to understanding risk, improving readiness and supporting real-world decision-making.

Typical playbook topics include:

A. Suspicious Items

Purpose

This playbook provides clear and actionable steps for handling unattended or suspicious items in venues or events, ensuring the safety of attendees and staff while minimising disruption.

Key Considerations

- **Safety First:** Prioritise the safety of everyone over operational continuity
- **Stay Calm:** Avoid causing panic with overly alarming language or behaviour
- **Collaborate:** Work closely with the police and follow their advice or instructions

Resources

- **Templates:** Suspicious Item Reporting Form, Evacuation Script (see Chapter 4 Communications Plan Template of the DSC Toolkits)
- **Training:** Use ProtectUK's ACT Awareness e-learning for staff preparation
- **Refer to:**
 - NPSA guidance: <https://www.npsa.gov.uk/resources/npsa-evacuation-lockdown-and-invacuation-guidance>
 - See, Check and Notify (SCaN) <https://www.npsa.gov.uk/see-check-and-notify-scan>
- **Contacts:** Maintain an updated emergency contact list for local authorities and first responders

Identifying a Suspicious Item

Characteristics to Look For:

- Items left unattended for an extended period
- Out-of-place or unusual packaging (e.g: wires, batteries, or excessive tape visible)
- Strange odours or leaking substances
- Notes or messages attached that suggest intent to harm

Questions to Ask:

- Has anyone claimed the item?
- Does the item look deliberately hidden or out of place?
- Is the location of the item consistent with a possible threat (e.g: near crowds or critical infrastructure)?

If the answer to any of these questions raises concerns, treat the item as suspicious

Immediate Actions

- **Do Not Touch the Item:**
 - Do not handle, move, or tamper with the item.
 - Keep a safe distance of at least 15 metres if possible.
- **Evacuate the Immediate Area:**
 - Clear the area around the item, directing people calmly away.
 - Avoid using mobile phones or radios near the item, as they could trigger certain devices.
- **Secure the Area:**

- Establish a cordon using barriers, tape, or other visible markers.
- Use natural cover or existing structures to enhance safety.

Notify Authorities

- Contact the police immediately by dialling **999**.
- Provide clear and accurate information:
 - Location and description of the item.
 - Actions already taken to secure the area.
 - Estimated number of people in the vicinity.

Communicate with Staff and Attendees

- Use clear and calm announcements to provide instructions:
 - Example: *“For your safety, we are temporarily closing this area. Please follow staff instructions and move to the designated safe zones.”*
- Ensure all staff are aware of the situation and follow predefined roles.

Post-Incident Actions

- **Await Clearance:**
 - Follow the advice of emergency services (who may not actually attend due to resources) before re-entering the area.
- **Debrief and Document:**
 - Conduct a post-incident review with all involved staff to discuss:
 - What was handled well
 - Areas for improvement
 - Record details in an **Incident Report Form** (see [Incident Reporting Template](#)) for future reference and training
- **Reassure Attendees:**
 - Provide clear communication to attendees after the incident, ensuring transparency and trust
- **Recovery** - Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations.

B. Improvised Explosive Device (IED) Scenario

Purpose

This section provides clear, actionable steps for responding to a suspected or confirmed Improvised Explosive Device (IED) incident, focusing on safeguarding lives, minimising risks and effective coordination with emergency services

Consider what actions to take if items are discovered during a bag search at an entry point to your event or venue.

Recognising an IED Threat

Potential Indicators of an IED:

- **Unattended or Suspicious Items:**
 - Unusual wires, switches, batteries, or tape visible
 - Items deliberately concealed in high-traffic or critical areas
- **Vehicles as Threats:**
 - Parked vehicles left in unusual locations for extended periods
- **Verbal or Written Threats:**
 - Bomb threats communicated directly or indirectly

Immediate Questions to Assess the Threat:

- Has the item or vehicle been reported as suspicious by staff or attendees?
- Does the item or situation seem deliberately out of place?
- Are there visible or audible signs of danger (e.g: audible ticking, leaking substances)?

Key Considerations

- **Safety First:** Never attempt to touch or move a suspicious item
- **Stay Calm:** Avoid causing panic during evacuations by using clear, calm instructions
- **Follow-Up:** Use the incident as a learning opportunity to strengthen future preparedness

Immediate Actions

Step 1: Avoid the Area

- Maintain a safe distance of at least 100 metres, increase this distance if the object appears large or contains unusual materials

Step 2: Evacuate Safely

- Move attendees and staff away from the suspected device using designated evacuation routes
- Avoid using routes that pass near the suspicious item or area
- Consider services that run above or beneath the area

Step 3: Alert Authorities

- Call **999** immediately and provide:
 - A clear description of the item or threat
 - The exact location, including nearby landmarks or access points

- Estimated number of people in the vicinity
- You may be asked to remain on the line

Step 4: Establish a Cordon

- Use barriers, signage, or natural markers to secure the area
- Maintain the cordon until emergency services arrive and advise otherwise

Communication Advice for Mobile Phones and Radios

Why Communication Devices Pose a Risk:

- Mobile phones, radios and other wireless devices can emit electromagnetic signals that may accidentally trigger an explosive device

Best Practices:

- **Avoid Use Near the suspected IED:**
 - Do not use mobile phones, radios, or other communication devices within 15 metres of the suspected IED
 - Move to a safe location (at least 100 metres away) before making emergency calls or using radios
- **Use Wired Communication if available:**
 - Landlines or other wired communication methods are safer alternatives for reporting and coordination
- **Brief Staff on Risks:**
 - Inform all staff and volunteers of the dangers of using wireless devices near a suspected device
- **Emergency Services Guidance:**
 - Defer to emergency responders for further advice on safe communication practices during the incident

Communication Protocols

- 1. Internal:**
 - Inform all staff and volunteers of the incident and the cordoned area
 - Where required, instruct staff with specific roles to assist with evacuation while staying safe
 - Instruct other staff to stay away from the area if they do not have a specific role in response to the incident
- 2. External:**
 - Provide calm and clear instructions to attendees:
 - Example: *“For your safety, please evacuate the area calmly and proceed to the designated safe zone. Follow staff guidance.”*
- 3. Media Inquiries:**

- Refer all questions to the designated spokesperson or emergency services
- Do not speculate or provide unverified details

Post-Incident Actions

Step 1: Assist Emergency Responders

- Share all relevant information, such as:
 - When the item was first noticed
 - Actions taken prior to their arrival
 - Any observations about the item or suspect behaviours

Step 2: Evaluate the Site

- Wait for clearance from emergency services before re-entering the area

Step 3: Provide Support

- Offer medical or emotional support to anyone affected by the incident

Step 4: Review and Debrief

- Conduct a thorough debrief with staff and emergency services
- Update risk assessments and the Incident Response Playbook based on lessons identified
- Recovery - Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations

Preventative Measures

1. Staff Training:

- Train all personnel in recognising and reporting suspicious items or behaviours
- Include ProtectUK's **ACT Awareness e-learning** as part of mandatory training

2. Regular Inspections:

- Perform routine sweeps of the venue for unattended or suspicious items
- Ensure all staff are familiar with high-risk areas (e.g: crowded zones, access points)

3. Clear Signage and Messaging:

- Display "If You See Something, Say Something" posters to encourage vigilance
- Use PA systems to remind attendees to report suspicious items or behaviours

4. Collaborate with Authorities:

- Engage with local police or counter-terrorism teams for advice on IED risk mitigation

Supporting Tools

- **Templates:**
 - Incident Report Form (see [Incident Report](#))
 - Evacuation Map highlighting safe zones and routes
 - Use the JESIP and or (M) ETHANE reporting methodology (see <https://www.jesip.org.uk/> and refer to [Section Q](#) of this document and / or the DSC Toolkits)
- **Contacts:**
 - Updated emergency service and local police liaison details
- **Resources:**
 - Access to ProtectUK guides and ACT Awareness training materials

C. Hostile Reconnaissance

Purpose

This playbook outlines steps to identify, report and respond to hostile reconnaissance – that is when individuals observe or gather information about a venue or event to plan a potential attack. By addressing this behaviour early, venues can reduce risks and deter further action

Key Considerations

- **Safety First:** Avoid direct confrontation; focus on observation and reporting
- **Stay Calm:** Maintain normal operations unless instructed otherwise by authorities
- **Follow-Up:** Use the incident as a learning opportunity to strengthen future preparedness

Resources

- **Templates:** Incident Reporting Form, Staff Briefing Checklist
- **Training:** ProtectUK ACT Awareness or similar e-learning modules
- **Emergency Contacts:** List of local police and counter-terrorism hotlines

Preventative Measures

- **Staff Training:**
 - Train all staff on recognising hostile reconnaissance and using this playbook
 - Include ACT Awareness e-learning as a baseline requirement
 - Use the “Power of Hello”, a simple yet effective public safety tool that enables security teams to engage with those who would do us harm and those at risk of harm as part of a strategy of prevention. See:

<https://ctinsight.net/what-is-the-power-of-hello/>, this is an integral part of the CALM approach: Chat, Assess, Limit, Monitor explained below.

🌀 **Physical Security:**

- Use visible deterrents like CCTV cameras and signage indicating surveillance
- Position security personnel at key access points

🌀 **Access Control:**

- Restrict sensitive areas to authorised personnel and monitor access rigorously
- Use ID badges or passes for staff and volunteers

🌀 **Community Awareness:**

- Encourage attendees to report suspicious activity using the venue's communication channels.

Recognising Hostile Reconnaissance

Indicators of Suspicious Behaviour:

🌀 **Unusual Photography or Filming:**

- Repeatedly photographing or recording entrances, exits, security measures, or crowd behaviour
- Use of high-powered lenses or discreet filming devices
- Drone use that has not been cleared with you

🌀 **Social Media Auditors and Opportunistic Reconnaissance**

- Recent guidance from the UK National Protective Security Authority (NPSA) recognises an emerging behaviour seen on social media, where individuals (often called **Auditors** or Social Media Auditors) film, photograph, or livestream organisational sites, staff, and security infrastructure with the intent of generating online content. While this activity is lawful and does not necessarily imply hostile intent, the content they share may be exploited by adversaries for hostile reconnaissance. Organisations should adopt measured engagement protocols (for example, the CALM approach: Chat, Assess, Limit, Monitor), maintain professionalism, avoid revealing sensitive security details, and focus on conveying that robust protective measures (like CCTV or access control) are present without over-explaining security configurations.

🌀 **Loitering in Restricted or Sensitive Areas:**

- Spending excessive time near access points, security barriers, or areas where they don't seem to have a legitimate purpose

🌀 **Repeated Visits:**

- Returning to the venue multiple times without clear justification, particularly at different times of day

🌀 **Overt Questioning:**

- Asking detailed questions about security procedures, event timings, or staff routines

🌀 **Suspicious Note-Taking or Mapping:**

- Drawing layouts or making notes about infrastructure, security positions, or crowd flows

Immediate Actions

🌀 **Observe and Assess:**

- Where safe to do so - use the “Power of Hello” as a tool to passively engage with the individual(s) – see above
- Note their appearance, behaviour and any tools or devices they are using

🌀 **Document Evidence:**

- Record the time, location and description of the activity
- Take note of physical identifiers such as clothing, height, or distinctive features
- If safe, capture your own discreet photos or videos for evidence

🌀 **Report to the Security Lead:**

- Notify the Responsible Person or the venue’s security team immediately
- Provide all documented details to help assess the risk

Escalation Process

🌀 **Internal Review:**

- The Security Lead reviews the report and decides on escalation based on the threat level
- If deemed credible, restrict access to sensitive areas and notify all staff to stay alert

🌀 **Contact Authorities:**

- For immediate concerns, contact the police via **999**
- For non-urgent but suspicious activities, call **101** or submit a report to **Counter Terrorism Policing** via the ProtectUK platform or call **0800 789 321**

Communication Protocols

🌀 **Staff Briefing:**

- Share details of the incident with all staff and volunteers
- Instruct them to remain vigilant and report any further unusual activities

🌀 **Public Announcements:**

- Avoid alarming attendees unless the situation escalates. Use non-disruptive language if necessary to adjust access or close areas

Post-Incident Actions

🌀 **Debrief and Record:**

- Conduct a debrief with all involved staff to review the response
- Complete a detailed incident report, including evidence gathered and actions taken

🌀 **Update Procedures:**

- Identify any vulnerabilities that may have been exploited during reconnaissance

- Adjust risk assessments, access controls, or training based on lessons identified
- **Follow-Up with Authorities:**
 - Share full incident details with police or counter-terrorism teams for further investigation and advice
- **Recovery:**
 - Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations.

D. Marauding Attacker - Knife / Gunman

Purpose

This playbook provides clear guidance for responding to an active attacker scenario involving a knife or firearm, prioritising the safety of attendees, staff and the public. It incorporates the **RUN, HIDE, TELL** principles promoted by UK counter-terrorism authorities

Key Considerations

- **Stay Calm:** Avoid panic to maintain control of the situation
- **Act Fast:** Every second counts in reducing harm
- **Follow Up:** Use the incident as an opportunity to strengthen future preparedness

Resources

- **Templates:** Incident Report Form, Staff Briefing Checklist
- **Training:** ProtectUK's ACT Awareness and Stay Safe training modules
- **Include:** Run, Hide, Tell posters around the venue
- **Emergency Contacts:** Updated list of local police and counter-terrorism hotlines

Preventative Measures

- **Staff Training:**
 - Ensure all personnel complete **ACT Awareness e-learning** and active attacker scenario training
 - Conduct 'Run, Hide. Tell' drills
 - Identify and communicate potential safe areas or refuges
- **Security Enhancements:**
 - Install physical barriers at key access points to deter attackers
 - Use CCTV to monitor high-traffic areas
- **Community Vigilance:**
 - Encourage staff and attendees to report suspicious behaviour proactively

Recognising the Threat

Potential Indicators of an Active Attacker:

- Individuals brandishing or using weapons in public areas
- Reports of shots fired or injuries consistent with a knife or gun attack
- Panic or sudden crowd movement toward exits

Immediate Questions to Assess the Situation:

- 🌀 Is there a visible or reported weapon?
- 🌀 Where is the attacker located?
- 🌀 How many attackers are there?
- 🌀 Are there injuries requiring immediate assistance?

Immediate Actions

RUN (Evacuate Safely if Possible):

- 🌀 Identify the safest escape route away from the attacker
- 🌀 Lead attendees to pre-identified evacuation points if it is safe to do so
- 🌀 Leave belongings behind to avoid delays

Staff Responsibility:

- 🌀 Direct attendees away from the danger and toward exits using calm but firm instructions
- 🌀 Avoid blocking exits or creating bottlenecks

HIDE (If Evacuation Is Not Possible):

- 🌀 Find a secure place to hide, such as a locked room or area with heavy furniture
- 🌀 Silence phones and stay quiet to avoid detection
- 🌀 Stay away from windows and doors; barricade the entry if possible

Staff Responsibility:

- 🌀 Guide attendees to hiding places, prioritising quiet and secure areas
- 🌀 Use available objects to barricade doors and reduce visibility

TELL (Call Emergency Services):

1. Call **999** as soon as it is safe to do so. Provide the following information:
 - Use (M) ETHANE reporting methodology. See <https://www.jesip.org.uk/> See [Section Q](#) of this document.
 - Location of the incident and the attacker
 - Description of the attacker(s) (e.g: clothing, weapons)
 - Number of injured persons and their locations

Communication Protocols

🌀 **Internal Communication:**

- Use radios or mobile messaging apps to update staff on the situation if safe
- Inform the Responsible Person (or tactical commander / authorised person) immediately

🌀 **External Communication:**

- Notify emergency services and cooperate fully with their instructions
- Avoid making announcements that could alert the attacker or cause further panic

Role-Specific Actions

🌀 **Responsible Person:**

- Coordinate the response, ensuring staff follow the plan
- Liaise with emergency services to provide updates and receive instructions
- The Police or Government Agencies may assume primacy when:

- A criminal act, such as a terrorist attack, is suspected
- Public safety or national security becomes the overriding concern
- Their resources or coordination are critical for effective management
- Refer to DSC Toolkit - Chapter 11 on Primacy and the 'Use the Memorandum of Understanding' to recognise the shift in who has control and establish roles and responsibilities
- **Security Team:**
 - Monitor access points to **prevent** further entry
 - Assist with evacuation or securing areas as directed
- **Staff and Volunteers:**
 - Follow the **RUN, HIDE, TELL** principles and assist attendees

Post-Incident Actions

- **Emergency Services Handover:**
 - Provide incident details, including attacker descriptions, witness accounts and injuries
- **Triage and Support:**
 - Administer basic first aid if trained and it is safe to do so
 - Provide emotional support to attendees and staff
- **Debrief and Review:**
 - Conduct a debrief with staff and emergency responders to identify successes and areas for improvement
 - Update the security plan based on lessons identified
- **Reassurance Communication:**
 - Issue a clear and transparent statement to attendees and stakeholders
- **Recovery:**
 - Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations.

E. Crowd Management Issues

Purpose

This playbook provides guidance for managing crowd-related issues, such as overcrowding, panic, or disorderly behaviour, to ensure safety and prevent escalation

Recognising Crowd Management Issues

Potential Indicators:

- Overcrowding at entry / exit points or high-traffic areas
- Sudden changes in crowd behaviour, such as pushing or surging
- Individuals exhibiting aggressive or disruptive behaviour

Questions to Ask:

1. Are crowd densities exceeding safe limits? **(these are preset limits on crowd density. Refer to guidance from resources such as the Purple Guide or Green Guide)*
2. Are there bottlenecks causing stress or frustration?
3. Is the situation escalating or showing signs of disorder?
4. Are barriers or fences being moved or circumvented by members of the public?

Preventative Measures

- Conduct pre-event assessments to identify potential congestion points
- Refer to previous event history, lessons identified
- Train staff in basic crowd psychology and de-escalation techniques
- Use barriers to guide flow and prevent bottlenecks

Immediate Actions

1. **De-escalate and Direct:**
 - Use marshals or staff to guide the crowd calmly to less congested areas
 - Remove disruptive individuals if safe to do so
 - Use marshals to report activity on the ground rather than relying on hearsay
2. **Redistribute Attendees:**
 - Open additional entry / exit points if available
 - If safe to do so break fence lines to allow the crowd to move away from the area (risk assess and consider whether the crowd will enter another unsafe area)
 - Use signage and announcements to redirect flows
3. **Call for Assistance:**
 - If the situation escalates, involve security personnel or police

Communication Protocols

- **Internal:** Use radios or messaging apps to alert all staff to the issue
- **External:** Notify attendees using clear, calm announcements:
 - Example: *"For your safety, please follow staff instructions and use the alternative exits provided."*

Post-Incident Actions

1. **Debrief Staff:**
 - Identify what caused the issue and how it was resolved
2. **Review Procedures:**
 - Update crowd control plans based on lessons identified
3. **Recovery:**
 - Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations.

F. Mass Casualty Event

Purpose

This playbook outlines the steps for managing a mass casualty event, ensuring swift response and coordination with emergency services.

Recognising a Mass Casualty Event

Potential Indicators:

- Multiple injuries due to incidents such as an attack, structural failure, or stampede
- Overwhelmed medical resources

Immediate Questions:

1. What caused the injuries?
2. Are emergency services needed immediately?
3. What other resources may be needed?
4. Is the area safe to enter for assistance?

Preventative Measures

- Ensure first aid kits and trained personnel are available
- Conduct drills for mass casualty scenarios
- Establish clear communication protocols with local hospitals and emergency services

Immediate Actions

1. **Call Emergency Services:**

- Dial **999** immediately and provide details of the incident, including:
 - Use (M) ETHANE reporting methodology. See <https://www.jesip.org.uk/> See also [Section Q](#) of this document.
 - Number of injured.
 - Location and access points.
 - Description of the event.

2. **Administer Basic First Aid:**

- Trained staff or volunteers should assist within their capabilities.

3. **Establish a Triage Zone:**

- Designate an area for grouping the injured by severity until emergency responders arrive.

Communication Protocols

- **Internal:** Notify all staff to assist or clear the area as needed.
- **External:** Use announcements to inform attendees and prevent panic:
 - Example: *“Medical assistance is on route. Please remain calm and follow staff instructions.”*

Post-Incident Actions

1. **Coordinate with Emergency Responders:**

- Provide full incident details and assist with evacuation of the injured.

2. Review and Report:

- Document the response and identify gaps for improvement.

3. Recovery:

- Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations.

G. Adverse or Severe Weather

Purpose

This playbook provides steps for handling severe weather events, ensuring the safety of attendees and minimising disruptions.

Consideration should also be made for events or venues where exposure levels need to be managed: such as for Ice Rinks, Christmas Fairs etc. The HSE, through the Workplace (Health, Safety and Welfare) Regulations, identifies minimum temperatures for workers for both indoor and outdoor settings while at work or in welfare spaces. Consideration should also be made for attendees; especially those who may be vulnerable or less able.

Recognising Adverse or Severe Weather Risks

Common Risks:

- ⊗ Lightning, high winds, heavy rain, flooding, extreme heat / cold, snow load on trees or structures.

Immediate Questions:

- ⊗ How will the weather impact safety (e.g: structural integrity, falling debris, slippery surfaces, blocked access, steep or narrow roads and pathways)?
- ⊗ Should the event continue or be delayed?
- ⊗ Are emergency shelters needed?
- ⊗ Is emergency access able to be maintained?

Preventative Measures

- ⊗ Monitor weather forecasts leading up to the event
- ⊗ Know the tolerance for all structures on site, the actions (and action levels) prior to and when these tolerances may be exceeded (see section below). Installers are required to provide clear documentation on the tolerances and actions to take.
- ⊗ Monitor vegetation, especially trees
- ⊗ Identify safe zones for sheltering attendees
- ⊗ Train staff on responding to specific weather-related hazards
- ⊗ In the case of snow and ice - be prepared to grit or clear areas to maintain access
- ⊗ Have on hand equipment such as buckets, shovels, saws and chain saws, axes etc

Key Weather Conditions to Monitor

- ⊗ **Wind Speed:**

- Thresholds for safe operation depend on the design and materials of the structure, typically specified by the manufacturer or installer

 Rainfall Intensity:

- Prolonged heavy rain can lead to pooling on roofs, causing collapse risks
- Heavy rain can lead to flooding of walkways, traffic routes and car parks

 Snow and ice:

- Prolonged snow can exceed tolerances for roofs or canopies, causing collapse risks, trees may become overloaded and drop branches and limbs
- Heavy snow can lead to blocking of walkways, traffic routes and car parks
- Formation of ice can restrict access and cause dangerous surfaces
- Water supplies may freeze
- Melting snow and ice may cause flooding

 Lightning:

- Increases the risk of strikes on tall or conductive structures

 Temperature Extremes:

- Can affect structural materials (e.g: expansion, brittleness)
- Can impact staff and attendees

Action Levels and Corresponding Responses

Normal Operations

- **Condition:** Weather conditions are within normal parameters (e.g: low winds, no extreme precipitation).
- **Actions:**
 - Bear in mind you may have more than one structure on site and that structures will have their own unique characteristics and tolerances, refer to the installer / hirers documentation.
 - Carry out routine visual inspections for wear, damage or deterioration of structural components, ties / guys, anchors, ballast systems and fabric or membrane coverings.
 - Ensure that drainage systems, adjacent ground conditions and ballast / anchorage arrangements remain clear, secure and functional (recognising that heavy rain or flooding may loosen anchorages or reduce ground bearing capacity).
 - Review that weather-monitoring equipment (anemometer or other site sensors) and trigger levels are functioning and calibrated.
 - Ensure that staff are aware of the protocols for weather monitoring, the agreed action levels and have received a briefing on potential escalations.
 - Use a decision log to record findings, actions considered and actions taken (e.g: use an Incident Management System)

Level 1 - Adverse Weather Warning

- **Condition** - Warning of: Moderate snow, winds, rain, or temperature changes predicted (e.g: wind speeds nearing structure's operational threshold).

- **Actions:**

1. Conduct an inspection of all structures, checking:
 - Anchoring systems (e.g: stakes, ballast).
 - Tension on tent or marquee fabric.
 - Stability of poles and supports.
2. Secure loose items near structures (e.g: signage, equipment).
3. Brief staff on monitoring protocols and prepare for possible escalation.

Level 2 - Adverse Weather Risk

- **Condition** – Adverse Weather at 50% of operational threshold.

- **Actions:**

1. Conduct a detailed inspection of the structure(s) (ideally by a competent person) focusing on:
 - Anchorage systems (stakes, ballast, ground fixings) for signs of looseness, movement or reduced capacity.
 - Tension and condition of guy wires, tie-backs, roof / membrane fabric (especially for catenary loads, ponding potential, or potential slackening after rainfall).
 - Stability of supports, poles, frames and connections (checking for deformation, separator fatigue or wear at joint fixings).
2. Secure all loose items in the vicinity of the structure (e.g: signage, equipment, temporary furniture) that could become wind-borne or impact the structure.
3. Re-brief and put on standby event personnel (including stewards, site supervisors) on the protocols: monitoring wind / gust velocities, identifying early signs of structural distress (e.g: fabric fluttering, ponding, anchor uplift) and preparing for potential escalation to Level 3.
4. Consider restricting certain non-critical operations
5. Consider reducing wind load exposure.
6. Posture for emergency shelter or evacuation routes.

Level 3: Severe Weather Risk

- **Condition:** Snow, winds, rain, or other conditions near the operational threshold of the structure (e.g: wind gusts at 75% of max tolerance).

- **Actions:**

1. Suspend non-essential activities in and around the structure(s); minimise occupancy to essential operations only and restrict access as appropriate.
2. Implement access control and cordon off the area around the structure(s) to prevent public or non-essential staff exposure to potential failure zones (including anchor uplift, guy-rope failure or fabric tear).
3. Consider areas downwind of the structure(s) where you may need to create an exclusion zone.
4. Activate continuous monitoring of weather updates and on-site structural behaviour: log real-time gusts, check anchor uplift, tension changes in

guys, ponding of fabric, settlement. Use a handheld anemometer (from a safe distance).

5. Notify the Responsible Person (e.g: Event Safety Manager)
6. Consider advising the hirer or installer of potential evacuation or need to dismantle.

Level 4: Immediate Hazard

- **Condition:** Weather conditions reach 90% of or exceed the structure's operational threshold, or structural integrity is visibly compromised (e.g: buckling, tearing fabric).
- **Actions:**
 1. Evacuate the structure and surrounding zone immediately; all occupants must be moved to pre-designated safe areas.
 2. Where safe and feasible, initiate controlled collapse or dismantling procedures in accordance with the manufacturer's method statement and by competent personnel.
 3. Notify emergency services if there is a significant risk to life or property (e.g: structural collapse imminent, large crowd present).
 4. Conduct head-count and ensure all attendees, staff and contractors are accounted for in safe zones; activate the incident-management communication plan (including internal and external messaging).
 5. Post-incident: secure the site, prevent re-entry until formal inspection and certification by a competent structural engineer or contractor.

Immediate Actions

1. **Assess the Situation:**
 - Monitor weather reports and actual conditions on-site.
 - Keep a record of weather readings
 - Keep a decision log of checks and actions considered / taken
2. **Implement Safety Measures:**
 - For lightning: Suspend outdoor activities and move people indoors or to designated shelters.
 - For high winds: Secure loose items and close exposed areas, monitor anchors / guys.
 - For flooding: Redirect attendees away from water-logged areas. Ensure that footings and anchors are not compromised by ponding or ground softening.
3. **Evacuate or Shelter:**
 - Move attendees to safe indoor locations if conditions worsen. Ensure evacuation routes remain clear and accessible.

Communication Protocols

- **Internal:** Alert staff to the weather risks and implement contingency plans.
- **External:** Inform attendees of any changes or safety instructions:

- Example: *“Due to severe weather, please proceed to the designated shelter area. Follow staff instructions.”*
- Example: *“Due to worsening weather conditions, this area is being closed for your safety. Please follow staff to designated safe zones.”*

Post-Incident Actions

Inspect for Damage:

- After the weather subsides, assess all structures for safety before resuming operations

Repair or Replace:

- Address damage promptly to avoid future risks

Debrief and Update Plans:

-  Review the incident response and update action levels as needed

Recovery:

- Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations.

Supporting Tools

-  Manufacturer specifications for operational thresholds
-  Inspection checklists for temporary structures
-  Weather monitoring apps or equipment (anemometer, rain gauge, ground-moisture sensors)
-  Emergency equipment and stockpiles
-  Decision log / Incident Management System

H. Hazardous Materials (HAZMAT)

Purpose

This playbook provides structured steps for identifying and responding to incidents involving hazardous materials, such as chemical spills, unknown powders, or gas leaks, to minimise risk to attendees, staff and the environment:

Recognising a HAZMAT Incident

Potential Indicators:

-  Strong, unusual odours
-  Visible spills, leaks, or powders in unusual locations
-  Reports of sudden illness or irritation (e.g: coughing, dizziness) among attendees or staff
-  Unmarked or improperly stored containers with chemicals

Immediate Questions to Assess the Situation:

-  Are there known HAZMAT's already stored on site, if so where?
-  What is the source of the material?

- ⦿ Are there visible signs of danger (e.g: fumes, skin irritation)?
- ⦿ Is the area safe to approach for further inspection?

Key Considerations

- ⦿ **Safety First:** If you think someone has been exposed to a hazardous substance, use caution and keep a safe distance to avoid exposure yourself.
- ⦿ Do not attempt to handle or remove hazardous materials without proper training and equipment
- ⦿ **REMOVE:** Remove yourself / the patient away from the hazard to avoid further exposure
- ⦿ **Act Quickly:** Minimise exposure by isolating the hazard and evacuating immediately
- ⦿ **Follow-Up:** Use incidents as learning opportunities to strengthen future preparedness

Preventative Measures

- ⦿ **Storage and Labelling:**
 - Clearly label and securely store any hazardous materials used at the venue (e.g: cleaning agents, fuels)
 - Maintain an up-to-date inventory of on-site hazardous substances
 - Maintain a COSHH (Control of Substances Hazardous to Health) register. See <https://www.hse.gov.uk/coshh/>
- ⦿ **Training:**
 - Train staff on HAZMAT identification and response procedures
 - Include HAZMAT awareness in routine safety drills
- ⦿ **Monitoring:**
 - Conduct regular checks of storage areas and event sites for potential hazards
 - Use detection equipment for larger venues if applicable (e.g: gas monitors)
- ⦿ **Emergency Supplies:**
 - Stock PPE (personal protective equipment) such as gloves, masks and eye protection for emergency use
 - Maintain spill kits designed for chemical containment

Immediate Actions

Step 1: Avoid Exposure

- ⦿ Do not touch, inhale, or attempt to clean up the material
- ⦿ Isolate the area by establishing a cordon (at least 15-30 metres) around the suspected hazard, or follow recommended distances for known HAZMAT's on site

Step 2: Evacuate the Area

- ⦿ Move all individuals away from the hazard calmly and quickly
- ⦿ Identify a safe zone upwind or away from the suspected material to minimise exposure

Step 3: Alert Authorities

- ⦿ Call **999** immediately and provide:

- Use (M) ETHANE reporting methodology. See <https://www.jesip.org.uk/>. See also [Section Q](#) of this document.
- Description of the material (appearance, smell, or effects observed)
- Exact location and any affected individuals
- Actions already taken (e.g: area secured, evacuation)
- In an emergency, stay on the phone until the emergency service(s) arrive(s) and follow any other advice given by the call handler to avoid further injury

Step 4: Secure the Scene

- Prevent unauthorised access to the area until emergency responders arrive
- Use signage, tape, or barriers to mark the hazard zone

If you have been affected:

REMOVE yourself from the hazard to avoid further exposure

- move away from the hazard as safely as you can. Do not delay
- it is important for the safety of yourself and others that you continue to stay away from the hazard
- if the skin is itchy or painful, access to a water source is essential to remove as much substance from the skin as possible and reduce further harm

REMOVE outer clothing if affected by the substance

- remove outer clothing to reduce possible further contact with any trapped substance by up to 80%. If safe to do so, bag up and / or leave contaminated items in situ to prevent further spread
- be very careful not to touch or spread the substance as this could lead to further injuries to the affected person or those helping them
- use gloves or other protective materials to cover hands and, if possible, carefully cut away clothing such as T-shirts, rather than pulling them off over the head
- by avoiding clothing coming into contact with the face, it reduces the risk of the substance getting into eyes, mouth and nose
- do not pull off any clothing stuck to the skin as it may damage that skin. A trained medical professional will remove when safe to do so
- the discarded clothing may present a hazard to anyone nearby as it may be covered in or have absorbed the substance and may give off harmful fumes or particles
- do not smoke, eat or drink

REMOVE the substance from skin if affected

- If the substance is painful or itchy:
 - do not wipe the skin as this may spread contamination or cause further harm
 - rinse the affected area continuously with clean water as soon as possible to remove any residual substance

- try to make sure the water can run from the affected area without pooling on the skin and potentially spreading the substance to a wider area
- If the substance is not painful or itchy:
 - REMOVE the substance using a dry absorbent material to soak it up or brush it off

When should you use the REMOVE advice?

- if you think you have been deliberately or accidentally exposed to a hazardous substance
- if you think you have been attacked with an acidic or corrosive substance

Sometimes the signs and symptoms of exposure are not obvious. These 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

Communication Protocols

- **Internal:**
 - Notify all staff using radios or messaging systems
 - Brief staff on the nature of the incident and areas to avoid
- **External:**
 - Announce safety instructions to attendees without causing panic. Example: *“For your safety, we are temporarily closing this area. Please follow staff instructions and proceed to the safe zone.”*

Post-Incident Actions

- **Assist Emergency Responders:**
 - Provide any known details about the material or the incident
 - Offer access to site maps or records of stored chemicals (if applicable)
- **Medical Assistance:**
 - Monitor individuals for symptoms of exposure and provide first aid within trained capabilities
 - Record details of affected persons for follow-up care
- **Debrief Staff:**
 - Review the incident and response with all involved personnel to identify successes and areas for improvement
- **Clean-Up and Recovery:**
 - Only trained professionals or certified contractors should handle HAZMAT clean-up
 - Ensure all materials are disposed of following environmental and legal guidelines
- **Recovery:**
 - Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations.

Supporting Tools

- **Templates:** Incident Reporting Form for HAZMAT incidents, Staff Briefing Checklist
- **Training Resources:** Access to ProtectUK or local authority HAZMAT training materials
- **Contact Information:** List of local HAZMAT specialists or contractors for post-incident recovery

Some other responses you may wish to consider:

I. Lost or Missing Person (See also DSC Lost or Vulnerable Persons Procedures)

Purpose

This section provides clear guidance for responding to reports of lost or missing persons at events, focusing on ensuring safety, minimising distress and efficiently locating the individual

Recognising a Lost or Missing Person Situation

Potential Scenarios:

- A child separated from their parent or guardian
- An attendee unable to locate a group member
- A vulnerable adult (e.g: someone with cognitive impairments) reported missing
- A person reporting themselves estranged from a carer or group

Questions to Gather Information:

1. Who is missing (name, age, physical description)?
2. When and where were they last seen?
3. Were there any suspicious circumstances?

Immediate Actions

Step 1: Gather Details / conspicuity

- Collect information about the missing person, including:
 - Name, age and clothing description.
 - Any specific needs (e.g: medical conditions, disabilities).
- If safe to do so, return to the last place seen for a minimum of 10 minutes in case the individual(s) return

Step 2: Alert Staff

- Notify all staff, volunteers and security teams. Provide the person's description and last known location.
- Assign someone to monitor entry / exit points discreetly.

Step 3: Search the Area

- Conduct a systematic search of the area where the person was last seen.
- Designate staff to check common gathering spots, such as toilets, seating areas, or quiet zones.

Step 4: Use Appropriate Communication Channels

- See section on broadcasting names and details in the DSC Lost or Vulnerable Persons Procedures

Step 5: Contact Authorities (if Necessary)

- If the person is not located within a reasonable timeframe or there are safeguarding concerns (e.g: suspected abduction), contact the police immediately

Communication Protocols

- 1. Internal:**
 - Ensure all staff remain updated on the search progress
 - Use radios or group messaging apps to share updates
- 2. External:**
 - Maintain discretion to avoid causing unnecessary panic among attendees
 - Escalate to emergency services if the situation requires specialised assistance

Post-Incident Actions

- 1. Reunite and Reassure:**
 - Once the person is found, reunite them with their guardian or group and offer support as needed
- 2. Document the Incident:**
 - Record details of the incident and the actions taken in an incident report
- 3. Review Procedures:**
 - Conduct a debrief with staff to identify any areas for improvement
- 4. Recovery:**
 - Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations.

Preventative Measures

1. **Lost Person Stations:**

- Establish a centralised location for reporting and assisting with lost persons

2. **Wristbands for Children:**

- Provide wristbands at entry points for children to write guardian contact details

3. **Staff Training:**

- Train staff to remain calm and act efficiently during lost person scenarios

J. Vulnerable Person Assistance

Purpose

This section provides guidance on identifying and assisting vulnerable individuals at events, ensuring their safety and well-being while maintaining a supportive and professional approach

Who is a Vulnerable Person?

- A child without a guardian
- An individual with disabilities, cognitive impairments, or medical needs
- Anyone appearing distressed, disoriented, or unable to communicate effectively

Questions to Assess the Situation:

1. Does the person require immediate medical assistance?
2. Are they alone or separated from a guardian or carer?
3. Do they appear confused, upset, or unable to find their way?

Immediate Actions

Step 1: Engage Calmly

- Approach the individual with sensitivity and avoid alarming them.
 - Example: “Hello, are you okay? Can I help you find someone or somewhere safe?”

Step 2: Move to a Safe Area

- Escort the individual to a designated quiet zone or first aid point
- Ensure they are comfortable and reassure them that help is on the way

Step 3: Notify the Appropriate Personnel

- Inform the event's safeguarding officer, first aid team, or Responsible Person
- Share any relevant details about the person's condition or situation

Step 4: Contact Guardians or Carers

- If the person is separated from their group, use the provided information to locate their guardian or carer
- If the person cannot provide contact details, follow safeguarding procedures and involve the police if necessary

Communication Protocols

1. **Internal:**
 - Notify staff or volunteers to assist with identifying the guardian or carer
2. **External:**
 - Avoid sharing personal details publicly or alarming attendees
 - Work closely with emergency services if the situation requires escalation

Post-Incident Actions

1. **Reunite and Follow Up:**
 - Ensure the individual is safely reunited with their guardian or receives appropriate care
2. **Document the Incident:**
 - Record all details, including times, actions taken and outcomes, in an incident report
3. **Evaluate and Learn:**
 - Review the response to improve procedures for future incidents
4. **Recovery:**
 - Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations.

Preventative Measures

1. **Designated Safe Zones:**
 - Set up areas where vulnerable individuals can be brought for support.
2. **Clear Signage and Information Points:**
 - Ensure attendees know where to seek help if needed
3. **Staff Awareness Training:**
 - Train staff to recognise and assist vulnerable individuals with empathy and professionalism

K. Cybersecurity Breach or Digital Disruption

Purpose

This section outlines how to respond to a cybersecurity breach or digital disruption, ensuring swift action to protect systems, data and operations

Recognising a Cybersecurity Breach or Digital Disruption

Potential Indicators:

- Unauthorised access to systems or networks
- Unusual system behaviour (e.g: error messages, slowed functionality)
- Suspicious emails or phishing attempts
- Reports of attendee data being leaked or ticketing system outages
- Alert from Down Detector of known disruption above a set threshold

Questions to Ask:

- Which system(s) are affected?
- Is sensitive data at risk (e.g: attendee or payment information)?
- Is the disruption malicious (e.g: hacking) or technical failure?

Immediate Actions

- **Contain the Issue:**
 1. Disconnect affected devices or systems from the network to limit spread
 2. Suspend online ticketing or payment systems if compromised
- **Notify IT Support:**
 1. Contact your IT team or cybersecurity experts immediately
 2. Provide details of the issue, including error messages or suspicious activity
- **Assess Potential Risks:**
 1. Identify the data or operations affected
 2. Determine if the breach impacts attendee safety or event continuity

Communication Protocols

1. **Internal:**
 - Inform key staff of the issue
 - Limit access to sensitive systems or data until resolved
2. **External:**

- Avoid immediate public announcements unless necessary to protect stakeholders (e.g: advising attendees to avoid phishing attempts)

Post-Incident Actions

- **Investigate and Document:**
 - Work with IT specialists to identify the root cause of the breach
 - Document the timeline, actions taken and data affected
- **Notify Stakeholders:**
 - Inform affected individuals or organisations as required under GDPR (if personal data is breached)
- **Enhance Security Measures:**
 - Update software, implement two-factor authentication and train staff on cybersecurity awareness
 - Conduct testing and simulations so staff become aware of fake addresses, phishing etc
- **Recovery:**
 - Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations.

L. Fire or Smoke Detection

Purpose

This section provides guidance on responding to fire or smoke detection, ensuring safe evacuation and coordination with emergency services

Recognising a Fire or Smoke Incident

Potential Indicators:

- Visible flames or smoke
- Fire alarms activated
- Strong burning odours or rising temperatures

Questions to Ask:

- Where is the source of the fire or smoke?
- Are there immediate risks to life or critical infrastructure?
- Is this a pre-cursor action as part of a multi-layered attack?

Immediate Actions

- **Activate Alarms:**
 - Where possible, trigger fire alarms if not already active

 Evacuate the Area:

- Direct attendees to the nearest fire exit(s) and assembly points
- Prioritise evacuation over attempts to extinguish the fire
- Deploy firefighting team with resources if trained and available

 Contact Emergency Services:

- Dial **999** and provide the location, size and nature of the fire
- Use (M) ETHANE reporting methodology. See <https://www.jesip.org.uk/>. See also [Section Q](#) of this document.

Communication Protocols

 Internal:

- Ensure staff assist in guiding attendees to safety
- Assign personnel to check toilets and less-visible areas for stragglers

 External:

- Use calm, clear announcements: *“Please leave the building immediately via the nearest fire exit. Follow staff to the assembly point.”*

Post-Incident Actions

 Await Clearance:

- Only re-enter the venue when authorised by fire services or authorised person

 Debrief and Report:

- Document the incident and review the effectiveness of the evacuation plan

 Inspect Damage:

- Conduct safety checks on equipment and infrastructure before resuming operations

 Recovery:

- Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations.

M. Power Outage or Technical Failure

Purpose

This section outlines how to respond to power outages or critical technical failures, ensuring attendee safety and operational continuity

Recognising a Power Outage or Technical Failure

Potential Indicators:

- Sudden loss of electricity or lighting
- Malfunction of critical systems (e.g: access controls, PA system, ticketing)
- Failure of backup systems (e.g: generators)

Questions to Ask:

- What systems or areas are affected?
- Are there immediate safety concerns (e.g: darkness, crowd panic)?
- Have connected systems failed in a safe condition, will they restart in a safe manner?

Immediate Actions

- **Ensure Safety:**
 - Activate emergency lighting if available
 - Guide attendees calmly to well-lit areas or exits
- **Report the Issue:**
 - Notify on-site technicians or building management
 - If external (e.g: a regional power outage), contact the utility provider
- **Prepare for Evacuation:**
 - If the outage persists or impacts critical safety systems, initiate evacuation protocols

Communication Protocols

- **Internal:**
 - Assign staff to manage crowd safety and assist with navigation
- **External:**
 - Use megaphones or backup PA systems to inform attendees:
 - Example: *"We are experiencing a technical issue. Please remain calm while we address the situation."*

Post-Incident Actions

- **Restore and Inspect Systems:**
 - Confirm systems are fully operational before resuming activities
- **Debrief and Document:**
 - Record the cause, response and any disruptions in an incident report
- **Test Backup Systems:**
 - Conduct maintenance checks on generators, emergency lighting and other fail-safes
- **Recovery:**
 - Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations.

N. Dangerous Animal or Wildlife Intrusion

Purpose

This section provides steps for safely managing intrusions by dangerous animals or wildlife at events, ensuring minimal disruption and risk

Recognising a Dangerous Animal or Wildlife Intrusion

Potential Indicators:

- Presence of aggressive or stray animals (e.g: dogs)
- Wildlife intrusion (e.g: snakes, wasps, birds, vermin or larger animals)

Questions to Ask:

- Is the animal an immediate threat to attendees?
- Can the animal be isolated safely?
- Who does it belong to?
- Where has it come from?

Immediate Actions

- **Secure the Area:**
 - Isolate the animal or wildlife from attendees if possible
 - Direct attendees away from the area
- **Contact Appropriate Services:**
 - Notify animal control, pest control, or local wildlife services
- **Manage the Crowd:**
 - Use calm instructions to keep attendees safe and minimise panic

Communication Protocols

- **Internal:**
 - Alert staff to the location and nature of the intrusion
 - Assign personnel to cordon off the affected area
- **External:**
 - Avoid alarming language:
 - Example: *“For your safety, please avoid the [area]. Staff are handling the situation.”*

Post-Incident Actions

- **Remove Hazards:**

- Ensure the animal or wildlife is safely removed by professionals
- **Inspect the Area:**
 - Check for damage or remaining risks before reopening the area
- **Debrief and Document:**
 - Record the incident, response and outcomes in an incident report
- **Recovery:**
 - Consideration should be given not only to immediate response, but to recovery and the safe return to normal operations.

O. Handling Media and Press Attention

Purpose

This section provides guidance on managing interactions with the media during and after an incident. The goal is to maintain accurate, consistent messaging, protect the integrity of the response and avoid misinformation while demonstrating transparency and responsibility.

Key Benefits of Effective Media Handling

- Builds trust and confidence among the public, attendees and stakeholders.
- Minimises the spread of misinformation and speculation.
- Enhances the reputation of your organisation through professional crisis management.

When to Engage with the Media

- **During the Incident:**
 - **Limited Engagement:** Focus on internal communication and incident management first
 - **Essential Updates Only:** Issue statements if media inquiries are frequent or if public safety messages need to reach a broader audience
- **Post-Incident:**
 - **Reassurance:** Provide updates to reassure the public and stakeholders about safety measures and next steps
 - **Accountability:** Address public interest in the incident to demonstrate professionalism and a commitment to improvement
 - **Media-Driven Attention:** Respond to direct media inquiries to control the narrative and counter misinformation

Principles for Media Engagement

- **Accuracy:**
 - Ensure all information provided is factual and verified
 - Avoid speculating on causes, motives, or outcomes

 Clarity:

- Use simple, concise language to avoid misinterpretation
- Avoid jargon or overly technical terms

 Consistency:

- Designate a single spokesperson to ensure uniform messaging across all communications

 Sensitivity:

- Respect the privacy of those affected by the incident, especially victims and their families

 Alignment with Authorities:

- Coordinate with emergency services, law enforcement and regulatory bodies to align public statements

Designating a Spokesperson

- The spokesperson should be:
 - A senior representative (e.g: Responsible Person or Event Manager) with knowledge of the incident
 - Ideally trained in media handling and crisis communication
 - Use the <https://www.npsa.gov.uk/see-check-and-notify-scan> training specifically for Communications professionals
- Their role includes:
 - Delivering official statements to media outlets
 - Responding to questions with approved messaging
 - Deferring inquiries beyond their expertise to relevant authorities

Key Considerations Before Speaking to the Media

 Assess the Situation:

- Is the incident under control?
- Do you have sufficient verified information to share?

 Prepare Messaging:

- Stick to prepared key points and avoid deviating under pressure

 Determine the Audience:

- Who needs the information? (e.g: local community, event attendees, national audience)

 Choose the Channel:

- Issue statements via press releases, social media, or live briefings depending on the situation's urgency and reach

Avoiding Common Pitfalls

 Speculation:

- Do not speculate on causes or outcomes; stick to confirmed facts

 Over-Disclosure:

- Avoid sharing unnecessary details that could compromise security or investigations

 Conflicting Information:

- Ensure statements align with those from emergency services or regulatory bodies

Post-Media Engagement Actions

 Monitor Coverage:

- Track media reports to ensure accurate representation of your statements

 Correct Misinformation:

- Issue clarifications promptly if inaccurate information is reported

 Internal Debrief:

- Review the effectiveness of media engagement and identify areas for improvement

Dealing with Intrusive Media Attention

Intrusive press or media attention can include:

- Persistent questioning during sensitive moments
- Attempts to access restricted areas or approach victims
- Speculative reporting or spreading misinformation

While engaging with the press is often necessary, it's equally important to protect the privacy of individuals involved and maintain control over the narrative

Strategies for Managing Intrusive Media

 Set Clear Boundaries:

- Define areas where the press can and cannot operate
- Use signage and security staff to enforce these boundaries
- Politely but firmly redirect journalists attempting to access restricted areas

 Designate Media Zones:

- Allocate specific areas for press briefings or media interviews to minimise disruption elsewhere

 Control the Flow of Information:

- Provide regular updates through an official spokesperson or press releases to reduce speculative reporting
- Refer journalists to approved sources, such as emergency services or regulatory bodies, for information outside your remit

 Maintain Composure:

- Respond to provocative or inappropriate questions calmly and professionally

Example Scripts for Challenging Scenarios

A. Press Questioning During an Ongoing Incident

- **Scenario:** A journalist approaches a staff member for comment while an incident is unfolding
- **Response Script:**
"I'm sorry, but I'm not authorised to comment at this time. Please direct your questions to [Spokesperson's Name or Organisation]. Thank you for your understanding."

B. Handling Persistent Questions About Sensitive Topics

- **Scenario:** A reporter repeatedly asks speculative questions, such as "Who is to blame?" or "How did this happen?"
- **Response Script:**
"We are still gathering information and it would be inappropriate to speculate at this time. Our priority is ensuring everyone's safety. We will provide updates as soon as we have verified information."

C. Managing Attempts to Access Restricted Areas

- **Scenario:** A journalist attempts to enter a restricted area or approaches victims directly
- **Response Script (possibly via Security Staff):**
"This area is currently off-limits for safety and privacy reasons. Please move to the designated media zone where you'll receive updates."

D. Addressing Emotional or Inappropriate Questions

- **Scenario:** A journalist asks a question that could cause distress or compromise privacy, such as asking about victims' identities
- **Response Script:**
"Out of respect for those affected, we are not sharing personal details at this time. Our focus remains on providing support and ensuring safety."

E. Deflecting Questions You Cannot Answer

- **Scenario:** The media ask about technical or legal matters outside your expertise
- **Response Script:**
"I can't comment on that specific detail. I recommend contacting [Emergency Services / Authority Name] for further information."

Escalation Protocols

- **If Media Becomes Aggressive:**

- Alert the Responsible Person or security lead immediately
- Politely but firmly end the interaction and suggest they contact the designated spokesperson

 If Misinformation Is Spread:

- Issue a public correction via the spokesperson or press release
- Work with legal counsel if the misinformation risks reputational or operational harm

Preventative Measures

 Media Code of Conduct:

- Share a clear set of expectations with journalists attending the event (e.g: no access to restricted zones, respectful behaviour)

 Press Briefing FAQ:

- Anticipate likely questions and prepare concise answers to reduce impromptu inquiries

 Training Staff:

- Train all frontline personnel on how to redirect media inquiries professionally

Benefits of Managing Intrusive Media Effectively

- Safeguards the dignity and privacy of those involved in the incident
- Prevents operational disruptions during critical response efforts
- Strengthens your organisation's reputation by demonstrating professionalism

Media and Press Interaction Cheat Sheet

Core Principles

- 1. Stay Calm and Professional:**
 - Be polite, even when faced with difficult questions
- 2. Be Clear and Concise:**
 - Stick to verified facts; avoid speculation or over-explaining
- 3. Protect Privacy and Integrity:**
 - Prioritise the dignity and confidentiality of individuals involved

Quick Dos and Don'ts:

- **DO:**
 - Refer journalists to the designated spokesperson if you're not authorised to comment
 - Stick to prepared statements and key messages
 - Keep your tone neutral and non-confrontational
 - Correct misinformation politely if it arises during an interview
- **DON'T:**

- Speculate about causes, motives, or outcomes
- Offer personal opinions or off-the-record comments
- Disclose sensitive or unverified information
- Let reporters steer you away from your key messages

Essential Tools

- **Prepared Statements:**
 - Have key points ready for anticipated questions
- **Press Kit:**
 - Include contact details for the spokesperson, background information on the venue or event and any pre-approved messaging
- **Media Zone:**
 - Set up a designated area where journalists can be briefed or conduct interviews without disrupting operations

Emergency Contacts

- **Spokesperson Contact:**
- **Press Office Email / Phone:**
- **Police Press Liaison:**

Key Messaging to Remember:

- **Safety First:**
 - *“Our priority is ensuring the safety of everyone involved.”*
- **Transparency:**
 - *“We’ll share updates as soon as we have verified information.”*
- **Responsibility:**
 - *“We’re working closely with authorities to manage the situation effectively.”*

Scripts for responding to Common Scenarios

When Approached by a Journalist:

- **Response:**
“Thank you for your interest. I’m not the right person to comment, but our spokesperson, [Name], can provide you with accurate information. Please contact them at [contact details].”

When Press Asks for Sensitive Information:

- Response:
“Out of respect for those affected, I can’t share personal details at this time. Our focus remains on ensuring safety and supporting everyone involved.”

When a Reporter Asks a Leading Question:

- Example Question: *“Don’t you think this incident could have been prevented?”*
- Response:
“Our priority right now is ensuring everyone’s safety. Once we’ve fully reviewed the situation, we’ll provide further updates.”

When Misinformation is Highlighted:

- Response:
“I’d like to clarify that [correct information]. For the latest verified updates, please refer to our official communications.”

Dealing with Intrusive Media

- Politely set boundaries:
“This area is restricted for safety reasons. Please move to the designated media zone.”
- Redirect inappropriate questions:
“I can’t comment on that right now. Please contact our spokesperson for more information.”
- End interactions gracefully:
“Thank you for your questions. I need to return to managing the situation, but we’ll provide an update as soon as possible.”

Key Tips for Handling Interviews:

- **Prepare Beforehand:**
 - Know your key messages and stick to them
 - If time allows rehearse a few lines by yourself
- **Pause Before Answering:**
 - Take a moment to compose your thoughts, ensuring clarity and accuracy
 - The pause will also focus attention and set the pace of the interview

General Principles for All Interviews

1. **Prepare Key Messages:**
 - Know the top 3 points you want to communicate
 - Use clear, concise language to avoid misinterpretation
2. **Stay Calm and Composed:**

- Speak slowly and clearly, even under pressure
- Maintain a neutral tone and avoid defensive body language
- 3. **Control the Narrative:**
 - Bridge back to your key messages if the interviewer strays
 - Use phrases like “*What’s important to note here is...*” or “*Let me clarify...*”
- 4. **Avoid Speculation or Jargon:**
 - Stick to the facts and avoid technical terms unless necessary, explaining them simply
- 5. **Assume Everything Is On the Record:**
 - Never make off-the-cuff or off-the-record comments or attribute blame

P. Media Interview Cheat Sheets

1. Face-to-Face Interviews

Overview: Conducted in person, often with the interviewer and camera crew present

Key Tips:

- **Body Language:**
 - Sit upright, keep your hands visible and avoid fidgeting
 - Maintain good eye contact with the interviewer, not the camera
- **Delivery:**
 - Speak conversationally but with authority
 - Pause briefly before answering to gather your thoughts
- **Handling Interruptions:**
 - Politely hold your ground if interrupted:
“*If I may finish, it’s important to highlight...*”

2. Piece to Camera

Overview: The speaker addresses the camera directly, typically for a statement or announcement

Key Tips:

- **Focus:**
 - Look directly into the camera lens, as though speaking to an individual
- **Clarity and Brevity:**
 - Keep statements short and impactful, using simple language
- **Composure:**
 - Avoid unnecessary movements; stand or sit still with a calm, open posture

3. Phone Interviews

Overview: Conducted over the phone, often for radio or print media, where tone and content matter most

Key Tips:

- **Tone of Voice:**
 - Speak clearly and avoid sounding rushed
 - Your tone conveys as much as your words
- **Pacing:**
 - Use natural pauses to let the interviewer absorb your points
- **No Visual Cues:**
 - Since the interviewer can't see you, verbal clarity is crucial
 - Avoid filler words like "um" or "you know."
- **Prepare Notes:**
 - Keep a list of key points handy to refer to during the call

4. Down-the-Line Interviews

Overview: Conducted remotely, often for TV, where the interviewer is in another location and you look directly into a camera

Key Tips:

- **Focus on the Camera:**
 - Maintain your gaze directly on the camera lens, so you are speaking directly to the interviewer or audience
- **Posture and Appearance:**
 - Sit upright with neutral, non-distracting clothing (e.g: avoid busy patterns)
 - Try to hold your posture
- **Time Delays:**
 - Be patient when responding to avoid speaking over the interviewer
 - Wait for a clear pause before answering
 - Be aware, there could be delays in the transmission
- **Technical Setup:**
 - Ensure the camera is at eye level, the background is tidy with no sensitive or confidential information in view and lighting is flattering but not harsh

5. Closing the Interview

1. **Reiterate Key Points:**
 - Use the opportunity to summarise your main messages:
"Before we finish, I want to emphasise..."
2. **Maintain Professionalism:**

- End with a polite thank you, regardless of the tone of the questions

6. Final Do's and Don'ts

- **Do:**
 - Practice beforehand to build confidence
 - Dress appropriately for the setting
- **Don't:**
 - Over-answer or elaborate unnecessarily
 - React emotionally, even to provocative questions

Q. Joint Emergency Services Interoperability Principles (JESIP)

Purpose

This section introduces the **JESIP principles**, a national framework developed in the UK to ensure effective joint working between emergency services during major incidents. See <https://www.jesip.org.uk/>

It is advantageous for venues, event organisers and key personnel to understand these principals in how to coordinate with police, fire, ambulance and other responders:

1. What is JESIP?

The **Joint Emergency Services Interoperability Principles (JESIP)** provide a standardised approach to **multi-agency incident response**. Established after lessons identified from previous major incidents, JESIP ensures all emergency services and partners work together effectively, with clear communication, shared situational awareness and coordinated action

JESIP applies to incidents of any scale requiring a **multi-agency incident response**, including:

- Terrorist attacks
- Structural collapses
- Fires, floods, or severe weather events
- Public disorder or mass casualty incidents

2. The Five JESIP Principles

The JESIP framework is based on five key principles that underpin effective joint working:

1. Co-locate

- **What it means:** Key decision-makers from the responding emergency services and partners (e.g: event staff, security leads) must meet and work together at a single location near the incident scene
- **Why it matters:** Co-location promotes face-to-face communication and better situational awareness, allowing for faster decision-making

2. Communicate

- **What it means:** Use **clear, consistent and plain language** when communicating information between agencies and partners. Avoid jargon or assumptions
- **Why it matters:** Effective communication reduces misunderstandings and ensures everyone has a shared understanding of the incident and response plans

3. Co-ordinate

- **What it means:** Establish clear leadership and agree on priorities, objectives and roles for all responding agencies and partners
- **Why it matters:** Coordination ensures a structured and organised response, preventing duplication of efforts or gaps in action

4. Jointly Understand Risk

- **What it means:** Share information to jointly assess risks, hazards and threats to responders, the public and the environment. Use this understanding to plan an appropriate response
- **Why it matters:** Joint risk assessment prioritises safety for all and enables better decision-making under pressure

5. Shared Situational Awareness

- **What it means:** Develop a shared understanding of the incident, using tools such as **M / ETHANE reporting** (explained below). This ensures all responders have the same, up-to-date information
- **Why it matters:** Shared situational awareness enables unified decision-making and avoids confusion in a rapidly evolving situation

The declaration of a MAJOR incident is likely to be made by the emergency services, event organisers should only refer to a 'possible' MAJOR incident.

3. The M/ETHANE Model

To support shared situational awareness, the **M/ETHANE model** is a key part of JESIP. It provides a structured way to report incidents to emergency services and partners:

- **M – Major incident** declared (Yes / No)
- **E – Exact location** of the incident
- **T – Type of incident** (e.g: fire, explosion, structural collapse)
- **H – Hazards** present or suspected (e.g: fire, chemicals, risk of collapse)
- **A – Access** routes to the scene (e.g: safest entry / exit points)
- **N – Number** of casualties or potential casualties

- **E – Emergency services** required (e.g: police, fire, ambulance, specialist units)

Example M/ETHANE Report:

- Major incident declared
- Location: South Entrance of Venue X
- Type: Explosion with smoke and fire
- Hazards: Structural collapse risk
- Access: Use North Gate
- Casualties: Approx. 15
- Emergency services: Fire, ambulance, police required urgently

4. Why JESIP Matters for Venues and Events:

- **Preparedness:** You can work seamlessly with emergency services during major incidents
- **Clear Communication:** Your team knows how to relay accurate information using M/ETHANE reporting
- **Unified Response:** Venue staff, security leads and event managers understand their roles and can co-ordinate effectively with police, fire and ambulance services
- **Safety Focus:** Joint risk assessments prioritise the safety of attendees, staff and responders

5. Actions for Event Organisers

1. **Train Staff:** Ensure key personnel understand the JESIP principles and how to use ETHANE reporting
2. **Plan for Co-ordination:** Identify locations for co-located decision-making (e.g: a Command Centre or Control Point)
3. **Liaise with Emergency Services:** Before events, engage with local emergency responders to discuss JESIP protocols and incident response plans
4. **Include JESIP in Your Plans:** Integrate JESIP principles into your event safety documentation, incident response playbooks and tabletop exercises

R. Incident Reporting Template

- **Purpose:** Record and analyse security incidents to improve future preparedness
- **Key Fields:**
 - **Incident specifics:**
 - Date:
 - Time:
 - Time stood down:
 - **Location Details:** Where the incident occurred within the venue or event

- **Suggested Incident Categories:**
 - 1 Fire
 - 2 Security
 - 3 Crowd
 - 4 Venue
 - 5 Medical
 - 6 Lost Persons
 - 7 Information Security
 - 8 Property Damage
 - 9 Crime
 - 10 Near Miss
 - 11 Unspecified / TBC
 - **Decisions / Actions Taken:** Immediate responses and resolutions
 - **Support needed**
 - **Observations & evidence**
 - **Witnesses:**
 - Names
 - Contact details
 - **Attachments:** Yes / No
 - **Post-Incident Review:** Recommendations for preventing recurrence, lessons identified and an agreed process to transfer their status to lessons learned
- **Template for Lost Persons (see also DSC Lost or Vulnerable Persons Procedures):**
- Name, age and physical description of the person
 - Clothing details and any specific needs (e.g: medical conditions)
 - Time and location last seen
 - Any suspicious circumstances noted

S. Staff Briefing Checklist

- **Purpose:** To ensure that all event staff are fully briefed on operational roles, safety procedures and emergency protocols before the event begins.
- **Key Fields:**
 - **1. General Event Information**
 - Event name, date and location.
 - Key event timings (doors open, peak periods, closing time).
 - Expected attendance numbers.
 - Event layout, including entrances, exits, key areas (stage, VIP, first aid, etc.).
 - Event objectives and key stakeholders (organisers, security, contractors).

- Sale and distribution of Alcohol and licencing matters.
- **2. Staff Roles & Responsibilities**
 - Individual responsibilities and reporting lines.
 - Responsible Person & chain of command and escalation procedures (use of control room if applicable).
 - Designated Premises Supervisor (DPS) for alcohol and licencing matters.
 - Check-in and check-out procedures.
 - Code of conduct and customer service expectations.
 - Handling lost property and customer enquiries.
- **3. Health & Safety Procedures**
 - Location of first aid stations and medical support.
 - Identification of first aiders and designated safety officers.
 - Fire safety procedures and fire assembly points.
 - Crowd management protocols and safe capacities.
 - Heat stress and hydration reminders (for outdoor events).
 - Manual handling and lifting precautions.
 - Food hygiene protocols.
 - Permits to Work.
 - Vehicles and speed limits.
- **4. Security & Incident Response**
 - Entry procedures, ticketing (including ticket types) and accreditation checks.
 - Re-entry procedures (if any).
 - Prohibited items and bag search policies.
 - Identification of security staff and stewards.
 - Emergency evacuation routes and procedures.
 - Responding to medical emergencies and security incidents.
 - Suspicious packages and hostile reconnaissance awareness.
 - Communication channels and radio call signs.
 - Incident management and reporting / record keeping.
- **5. Emergency Procedures**
 - Alarm signals and emergency PA announcements.
 - Shelter-in-place and lockdown procedures (if applicable).
 - Lost or vulnerable person protocol.
 - Adverse and severe weather action plan (for outdoor events).
 - Coordination with emergency services (fire, police, ambulance).
 - Entry and escort of emergency vehicles.
 - Assembly points and evacuation leadership roles.
- **6. Communication & Briefing Confirmation**
 - Radio distribution and check-in.
 - Team WhatsApp or SMS text alert groups (if used).
 - Contact details for supervisors and key personnel.
 - Dealing with the Press or Media.
- **7. Round -up**

- Confirmation of briefing understanding (staff sign-off or roll call).
- Any last-minute updates or reminders.
- Provide any expectations for 'standing down' and any hot de-briefs before teams go off shift
- **Sign-Off Confirmation**
 - Attendance sheet and or confirmation staff have received the briefing and understand their responsibilities.

T. Suspicious Item Reporting Form

- **Purpose:** To ensure an accurate record is made should an item be found.
- **Include:**
- **Incident Details**
 - Date:
 - Time:
 - Location of Suspicious Item:
 - Reporting Staff Name:
 - Position/Role:
- **Description of Suspicious Item**
 - Size (Approximate Dimensions):
 - Shape: Box / Bag / Cylinder / Other:
 - Colour:
 - Material (Plastic, Metal, Fabric, etc.):
 - Any markings, labels, or writing on the item?
 - If yes, describe:
 - Sounds or unusual smells?
 - If yes, describe:
- **Discovery & Actions Taken**
 - How was the item found?
 - What was the last known safe walking route to and from the item?
 - Who was present when the item was found?
 - Was the area evacuated?
 - Has security been informed?
 - If yes, name of security officer informed:
 - Have emergency services been contacted?
 - If yes, time of contact:
 - Name of responding officer (if applicable):
 - Was the item moved or disturbed before reporting?
 - If yes, explain:
- **Additional Observations**
 - Was anyone seen placing or abandoning the item?

- If yes, description of person(s):
- Any suspicious behaviour in the area prior to discovery?
- If yes, details:
- CCTV coverage of the area?
- If yes, has security reviewed footage?

● **Reporting & Follow-Up**

- Reported to: Security / Event Control / Police / Other:
- Time of Report:

● **Actions Taken Post-Reporting:**

- Area Secured
- Immediate review of CCTV if available
- Awaiting Emergency Response
- Public/Staff Notified
- Other:

● **Sign-Off Confirmation**

- Reporting Staff Signature:

Instructions to staff:

- Do not touch or move the suspicious item.
- Refer to the Suspicious Item topic in the DSC Incident Response Playbook
- Keep people away from the area and follow evacuation protocols if necessary.
- Contact security or emergency services immediately.
- Record all details as accurately as possible to assist responders.

U. Draft Information Sharing Agreement (ISA) Template

For Use in Mutual Aid and Incident Response Collaboration

1. Purpose of the Agreement

This Information Sharing Agreement sets out the lawful basis, principles and safeguards for the sharing of personal and operational data between the parties listed below for the purpose of mutual aid, incident response and collaborative safety and security planning.

2. Parties to the Agreement

This agreement is between the following organisations:

[Party A]

Organisation Name

Contact Name & Role

Contact Details

[Party B]

Organisation Name

Contact Name & Role

Contact Details

[Optional Parties]

Each party is a data controller for the personal data it holds.

3. Legal Basis for Sharing

Data will be shared under the following lawful basis as defined by Article 6 of the UK GDPR:

- a) Legal obligation: To comply with health and safety or public protection duties.
- b) Vital interests: To protect the life of an individual in an emergency.
- c) Public task: Performance of a task carried out in the public interest or official authority.

Where special category data is shared, the additional legal basis under Article 9 shall be:

- d) Substantial public interest under DPA 2018 Schedule 1, Part 2.

4. Data to Be Shared

Data may include (but is not limited to):

- Name and contact details of Responsible / Accountable Persons
- Incident logs or witness reports
- CCTV or body-worn video footage
- Emergency planning documentation
- Crowd risk information or safeguarding concerns

5. Information Sharing Principles

All parties agree to:

- Share only the minimum necessary data for the stated purpose
- Maintain accuracy and timeliness of shared data
- Apply appropriate security controls (encryption, access controls)
- Maintain records of what data was shared and when

6. Retention and Deletion

Each party will retain shared data only for as long as necessary to fulfil the agreed purpose, subject to their own retention schedules. Any onward sharing must be consistent with the original purpose.

7. Data Subject Rights

Where applicable, each party will respect the data rights of individuals under UK GDPR, including:

- The right to be informed
- The right of access
- The right to rectification or objection (subject to exemptions in emergencies)

8. Security Measures

Each organisation confirms it has appropriate technical and organisational measures in place to:

- Prevent unauthorised access, alteration, disclosure, or loss
- Ensure availability of data during emergency operations

9. Breach Notification

If a personal data breach occurs, the party discovering it must:

- Notify affected parties without undue delay
- Cooperate in containment and reporting
- Follow their own ICO reporting obligations

10. Review and Duration

This agreement is valid for a period of 12 months from the date of signing or until replaced. It will be reviewed:

- After any major incident
- If data protection law changes
- Annually, as part of preparedness planning

11. Signatories

Signed on behalf of [Party A]:

Name: _____

Role: _____

Date: _____

Signed on behalf of [Party B]:

Name: _____

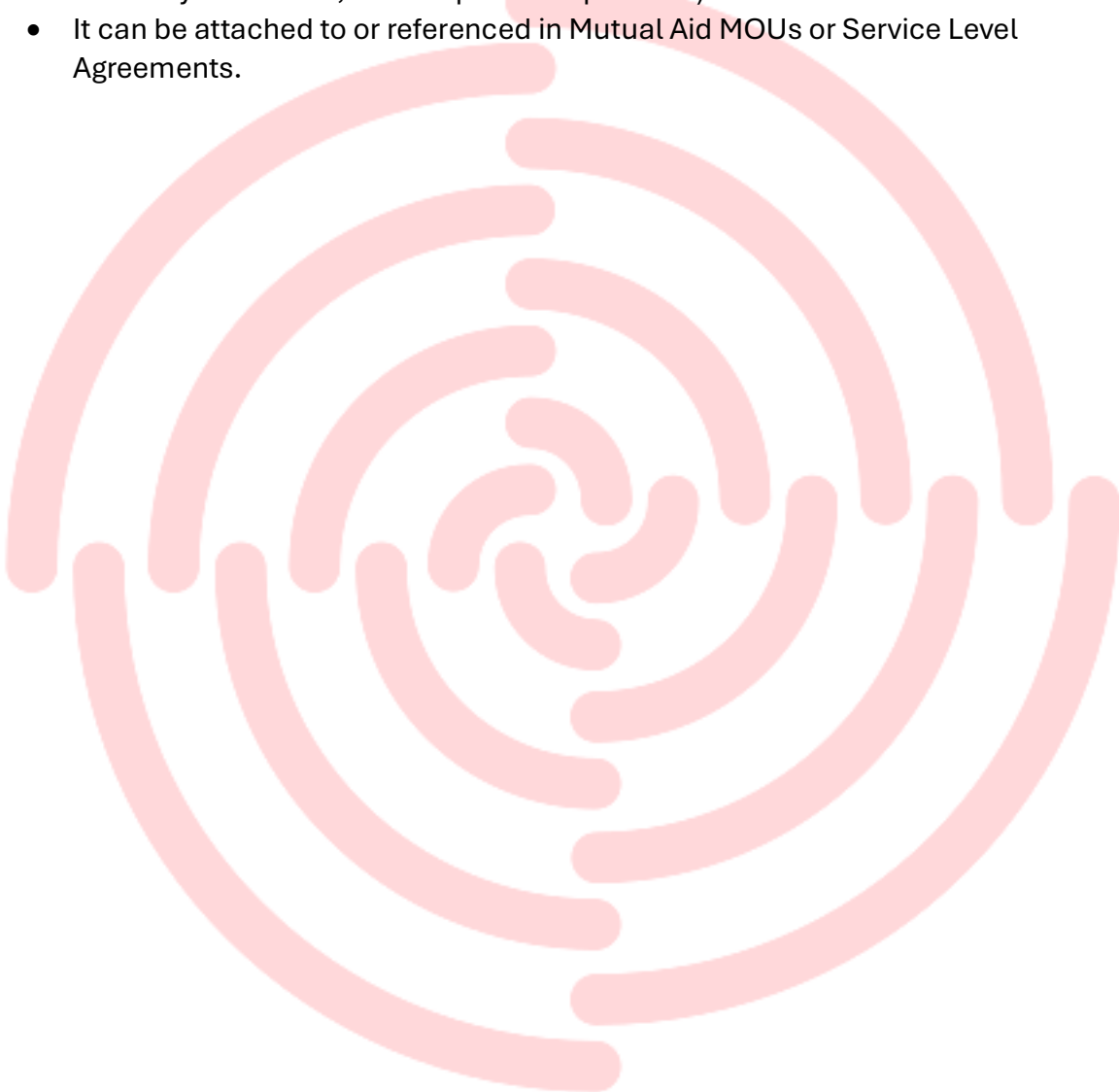
Role: _____

Date: _____

Other parties:

Additional Notes:

- This template can be adapted for specific use cases (e.g: between local authority and venue, or multiple event partners).
- It can be attached to or referenced in Mutual Aid MOUs or Service Level Agreements.



The legal bit: Decision Support Centre (DSC) & National Events Database (NED) Disclaimers

This Incident Response Playbook and associated resources, including the Events and Venues Toolkit and Responsible Persons Training materials, are provided for guidance only.

They are intended to support venues, events and organisations in developing a practical approach to preparedness, decision-making and incident response in real-world environments.

They do not constitute legal, professional or specialist advice, and should not be relied upon as a substitute for appropriate professional consultation where required.

While these resources have been developed with reference to current legislation and guidance, including the Terrorism (Protection of Premises) Act 2025 (Martyn's Law), they are not intended to provide definitive interpretation of legal obligations or regulatory requirements.

Users are responsible for ensuring that their approach reflects their specific circumstances, including the nature, scale and complexity of their venue or event.

No two environments are the same, and incidents may develop in ways that are dynamic, unpredictable and influenced by factors beyond immediate control. As such, the guidance provided should be applied with judgement and adapted as necessary.

The Decision Support Centre accepts no liability for any loss, damage or consequence arising from the use of, or reliance upon, these materials.

1. General Disclaimer

The Decision Support Centre (DSC) and National Events Database (NED) provide toolkits, playbooks and resources for informational purposes only. These materials do not constitute professional, legal, or regulatory advice. Users are encouraged to consult relevant experts (e.g: legal advisors, safety consultants) and ensure compliance with applicable laws, regulations and guidance (e.g: Terrorism (Protection of Premises) Act 2025, Health and Safety Act 1974, GDPR). The DSC and NED make no warranties or guarantees as to the accuracy, completeness, or applicability of these materials in specific circumstances.

The National Events Database is designed to support visibility across the events and venues ecosystem by providing a shared industry reference. It is intended to be a

resource that may be useful to organisers, authorities, insurers and industry stakeholders and does not imply formal data sharing agreements.

References to third-party organisations and resources are provided for information purposes only and do not imply endorsement, partnership or formal affiliation.

2. Limitation of Liability

The DSC and NED are not liable for any direct, indirect, incidental, consequential, or other damages arising from the use or misuse of the materials provided. Users assume full responsibility for implementing safety procedures, risk management plans and incident responses based on their individual circumstances and requirements.

3. No Guarantee of Outcomes

While every effort has been made to ensure the resources provided are practical and accurate, the DSC and NED cannot guarantee that the implementation of these materials will prevent incidents, injuries, or legal compliance failures. Users must apply their own judgement, adapt procedures as necessary and consult professionals where required.

4. User Responsibility

It is the sole responsibility of users to assess the relevance, suitability and implementation of the materials provided within their own operations, venues, or events. The DSC and NED are not responsible for verifying individual safety measures, risk assessments, or legal compliance obligations.

5. Third-Party Links or References

The toolkits and playbooks may include references to third-party resources or websites. The DSC and NED do not control, endorse, or take responsibility for the accuracy, completeness, or availability of third-party content. Users access such resources at their own discretion.

Mention of a third party is for explanatory context only and does not imply any existing contractual, operational, or data sharing relationship.

However, we encourage organisers and venues to make use of publicly available guidance and training resources. Useful publicly available resources include ACT Awareness e-learning available through ProtectUK.

6. Intellectual Property Disclaimer

All content, including text, diagrams, templates and resources within the toolkits and playbooks, is the intellectual property of the Decision Support Centre (DSC) unless otherwise stated. Users may reproduce and use the materials for non-commercial purposes within their own venues or events. Unauthorised reproduction, modification,

or distribution of these materials without prior written consent from the DSC is strictly prohibited.

7. Compliance with Regulations

The resources provided are intended to support venues and event organisers in implementing reasonable safety measures and best practices. Users must independently ensure compliance with relevant laws, regulations and guidance, including but not limited to the Health and Safety at Work Act 1974, the Terrorism (Protection of Premises) Act 2025 (Martyn's Law) and GDPR obligations.

8. Tailored Solutions Disclaimer

The toolkits and playbooks provide general guidance and templates for managing incidents, safety and compliance. These resources are not specific to any individual venue or event. Users must adapt and tailor the materials to meet their unique needs, risk profiles and operational requirements.