Developing a comprehensive incident management response plan

Guidance for faith institution leaders and managers

March 2015

This toolkit was developed using best practice in incident management and putting this in the context of local faith institutions. Our thanks go to the West Midlands key partners involved: faith institutions with their city and local councils in the following areas Birmingham, Coventry, Wolverhampton, Dudley, Sandwell, Solihull and Walsall, West Midlands Police and West Midlands Counter Terrorism Unit (CTU). The project was funded by Birmingham City Council via a Home Office grant.

Email: info@faithassociates.co.uk Web: www.faithassociates.co.uk Telephone: + 44 (0) 845 273 3903

With thanks to The Centre for the Protection of the National Infrastructure (CPNI) for giving permission to abstract the Planning and Preparing section of this toolkit from their publication *Counter Terrorism Protective Security Advice for Places of Worship* © ACPO 2009 available from http://www.nactso.gov.uk/crowded-places.

Welcome

This comprehensive guide provides more detailed guidance to help faith institutions prepare and respond to the situations faith institutions have deal with and maybe likely to deal with in the future. Before walking you through this guide take some time to consider the following questions:

- what an incident is?
- what incidents are your organisation likely to need to prepare for?

What is an incident?

An “incident” is any unexpected event or series of events that has the potential to or does negatively impact and/or harm the organisation’s staff, premises, congregations, service users, communities, finances, image and reputation and requires immediate senior leadership notification, focused involvement, action and resources. An incident can be a physical or non-physical event and even an emerging issue that threatens to cause damage or harm.

What incidents are your organisation likely to need to prepare for?

The following are a list of incidents or crises which may affect faith institutions and be cause for starting an incident management procedure:

- storm or flood
- industrial/domestic accident, fire or explosion
- violence within the organisations premises or locality
- act of terrorism
- hazardous material spill/release
- major release of pollutants
- civil disruption eg riot, sit in
- local or national industrial action or dispute
- malicious rumour or inaccurate media report
- major investigation local or national government agency
- legal action against the organisation
- significant or malicious threats to reputation
- alleged misbehaviour by management, staff or volunteers
- safeguarding concerns for a child, young person or vulnerable adult you provide services to.

Now, consider how your organisation would respond to the top two or three incidents. This guide can help you respond with sections covering:

- managing risk
- planning
- incident management policy (draft for customisation)
- response team including contacts
- concept of operations
- response plan
- training and exercises
- communications.

This guide and supporting resources are all available to download from www.faithassociatces.co.uk/im

Managing risk

Managing the risk of incidents happening is one responsibility when preparing contingency plans to respond to incidents likely to happen in or near places of worship which might affect public safety or disrupt services being provided.

Faith institution managers have a responsibility to plan and prepare to respond to incidents and minimise their impact under Health and Safety Regulations and the Regulatory Reform (Fire Safety) Order 2005 or in Scotland the Fire (Scotland) Act 2005 and Fire Safety (Scotland) Regulations 2006.

Law, liability and insurance

There are also legal and financial reasons why you should plan to respond to.

Criminal prosecution and heavy penalties under Health and Safety if it emerges that core standards and statutory duties have not been met. Especially relevant to protective security in places of worship are the specific requirements of the Health and Safety at Work Act 1974 and Regulations made under it to do all of the following:

- carry out adequate risk assessments and put suitable measures in place to manage those identified risks, even where they are not of your making and are outside your direct control: then be alert to the need to conduct prompt and regular reviews of those assessments and measures in light of new threats and developments
- co-operate and co-ordinate safety arrangements between owners, faith leaders, security staff, tenants and communities, including the sharing of incident plans and working together in testing, auditing and improving planning and response.
- ensure adequate training, information and equipment are provided to all staff, and especially to those involved directly in safety and security
- put procedures and competent staff in place to deal with imminent and serious danger and evacuation.

The tensions which might naturally arise within communities from time to time, must be left aside entirely when planning protective security

Insurance against damage to your place of worship to deal with the aftermath of an incident is generally available but typically at an additional premium. Adequate cover for loss of revenue and interruption of services during a rebuild or decontamination is expensive even where available from the limited pool of specialist underwriters. Full protection against compensation claims for death and injury to staff, worshippers and visitors caused by terrorism is achievable, albeit at a cost. With individual awards for death and serious injury commonly exceeding the publicly-funded criminal injuries compensation scheme upper limit, there is every incentive for victims to seek to make up any shortfall through direct legal action against owners, operators, managers and tenants under occupiers liability laws.

Business continuity

Business continuity planning is essential in ensuring that your faith community can cope with an incident or attack and return to **business as usual** as soon as possible. You can develop a basic plan which can be implemented to cover a wide range of possible incidents. For example, part of the plan will cover evacuation procedures, but the principles will generally be applicable for fire, flooding or bomb threat incidents. This is particularly relevant for places of worship in order that they might provide the support required by the communities they represent following an incident.

Reputation and goodwill

These are valuable, but prone to serious and permanent damage if it turns out that you gave a less than robust, responsible and professional priority to best protecting people against the effects of an incident. Being prepared and security minded can reassure your congregation and staff that you are taking their safety seriously.

Do you know who your neighbours are and the nature of their business? Could an incident at their premises affect your faith group? There is limited value in safeguarding your own premises in isolation. Take into account your neighbours' business plans and those of the emergency services.

A number of faith groups have adopted good practice to enhance the protective security measures in and around their premises. Places of worship differ in many ways including, size, location, staff numbers, layout and operation and some of the advice included in this toolkit may have already been introduced at some locations.

For specific advice relating to your place of worship, contact the nationwide network of specialist police advisers known as Counter Terrorism Security Advisers (CTSAs) through your local police force. They are co-ordinated by the National Counter Terrorism Security Office (NaCTSO).

Protective security

The best way to manage the hazards and risks to your place of worship is to start by understanding and identifying the threats, vulnerabilities and resulting impact.

This will help you to decide:

- what security improvements you need to make
- what type of contingency and security plans you need to develop.

For some places of worship, simple good practice – coupled with vigilance and well exercised contingency arrangements – may be all that is needed.

Risk management

If, however, you assess that you are vulnerable to attack, you should apply appropriate protective security measures to reduce the risk to as low as reasonably practicable. The following are the typical stages to follow in the risk management cycle.

1. Identify the threats.
2. Establish what you want to protect and your vulnerabilities.
3. Identify measures to reduce risk (security improvements/security plans).
4. Review your security measures and rehearse/review your security plans.

Full details and guidance on working through the risk management cycle is provided by the Centre for the Protection of the National Infrastructure (CPNI) in their publication Counter Terrorism Protective Security Advice for Places of Worship available from www.nactso.gov.uk/crowded-places. The section is based on section *Two, Managing risks* with their kind permission.

Planning

Your incident management and response capabilities should follow a standard approach. Here are the key activities to follow to build your Response Plan. The toolkit section includes guidance and forms to help.

1. Incident Management Policy

Draft an **Incident Management Policy** that includes a standard and set of expectations. These should then be reviewed and agreed by your organisation leadership team.

2. Response Team and their roles and responsibilities (use A3)

Agree who in your organisation will play an active role in dealing with an incident in a **Response Team**. The focus should be on team members who can provide practical and decision making support in areas such as human resources, finance, legal, health and safety, communications. A form to record details of your Response Team is provided at A3. Where you can, try to ensure there is a primary and alternate identified for each team role you decide to have.

3. Define Response Team relationships and local contacts

Record how the **Response Team** will provide incident and crisis management support for your organisation and how it will coordinate, communicate and integrate with local government and emergency services.

4. Create Concept of Operations

Review the key components agreed above and write them into a **Concept of Operations** (often abbreviated to **ConOps**) which defines the process and procedures for the **Response Team** will use to do its job eg team structure, response activation, Communications and coordination, managing issues and actions, resources.

5. Develop Response Plan

Review your existing Response Plan or draft your first plan using the guidance and concepts defined in this toolkit. If no plan currently exists for your organisation write one that covers the requirements set out in A5. Reference the integration, oversight and management considerations for any other incident response plans you may have such as procedures for emergency response, business continuity, IT disaster recovery, etc. Secure feedback and approval from your organisation's leadership as necessary.

6. Training and exercises

Arrange training and exercise activities to improve your incident response capabilities and test that the plan for your organisation works.

7. Communications guidance

Make time to think through and draft a set of key messages on the top two or three incidents you believe are most likely to impact your organisation. This will provide you with a good starting point should one of the incidents occur.

1. Incident Management Policy (draft for customisation)

This **Incident Management Policy** and plans are hereby created to establish an incident management process that will allow coordination and decision-making when an incident occurs or when incidents develop that could eventually become a crisis for the organisation. The incident management plans define a process for reporting and notification of incidents and establishing a Response Team to lead the management of an incident.

Our approach to Incident Management will help us make sure that we are doing our best to protect our staff, premises, congregations, service users and communities and our reputation. It gives us the capability to:

- secure and protect our staff, premises, congregations, service users and communities in a manner consistent with related laws and policies
- quickly and effectively respond to, manage and recover from incidents
- mitigate the impact of these risks on our staff, premises, congregations, services
- maintain the capabilities through ongoing planning, training, exercising, quality assurance and other maintenance activities.

Our Incident Management approach complements emergency and other incident response procedures and related activities. This Incident Management Policy supersedes any of our previous crisis management policies.

Incident management standard

Each of our premises must have a Site Response Plan in place. That plan should reference and incorporate guidance provided in this Incident Management Policy and should establish a fundamental response capability for the range of risks and threats we may face. These plans should include the framework for how we manage incident response and integrate and align any other response aspects including local government and emergency services response, business continuity, IT disaster recovery and other specialty or incident plans and procedures as needed.

Incident management expectations

Each of our premises should:

- establish a Response Team
- define relevant response sub-teams as appropriate eg fire wardens, floor warden/evacuation teams, etc
- include basic plan elements
- maintain and update plans with an annual review
- keep multiple copies of the plan available for use during an emergency, and maintain electronic or other access if appropriate
- train and exercise all Response Team members on a semi-annual basis or as defined
- participate in an annual self-assessment process designed to provide an assessment of the status of your program, and to provide a broader understanding and assessment of preparedness functions and capabilities.

Date adopted: XX/XX/20XX Date for review: [12 months after 'Date']

2. Response Team including contacts

Establishing a Response Team helps see and reduce the impact of a significant incident. This approach ensures coordinated response actions and ensures all involved have clear roles and responsibilities.

A Response Team should be activated to respond and manage all incidents. For most faith institutions this team should be used to respond to:

- physical emergencies incidents that pose an immediate threat to life, health or safety of persons and property providing an immediate and competent handling of such an incident
- for non-physical and non-emergency incidents.

Response Team responsibilities

- Assessing crisis impacts on the organisation.
- Forecasting consequences.
- Managing crisis issues.
- Selecting the strategy(ies) to manage the actual or anticipated consequences.
- Issuing policy directives for dealing with incident issues it is responsible for.
- Ensuring logging and coordination of incident issues and response actions and providing oversight of the response.
- Providing or coordinating the best available resource support and/or technical expertise.
- Coordinating the response activities.
- Supporting incident response including business continuity, resumption and recovery.
- Managing consequences stemming from the incident.
- Reporting incident information to agreed internal and external colleagues and organisations.
- Providing tactical response to site emergencies.
- Executing issues management response efforts.
- Executing business recovery plans.
- Restoring normal operations on premises.
- Communicating with locally affected parties and the public, including contractors, vendors, etc.

Contact details

Record the contact details of the Response Team, agreed internal contacts and local external contacts and ensure all relevant staff have access to a copy.

Note: a contact details template is available at www.faithassociates.co.uk/im to help you do this.

4. Concept of Operations

The Concept of Operations includes what can be done and the resources available. It should also include the level at which other help should be called on to provide additional support. The concept of operations should address the following five components:

- team structure
- activation
- communications and coordination
- open issues and action item status tracking
- response team resources.

When developed your Concept of Operations which defines the process for what will happen will be included in your Response Plan (see section 5).

Team structure

This section of your plan includes Response Team membership, roles and responsibilities of individual members. All team member contact information is typically in an appendix as a schedule.

Response activation

This section of your plan should define the circumstances and criteria under which the Response Team will activate, who is responsible for making that decision, and the process for activation of the response team.

Communications and coordination

Communications and coordination is essential to a successful response, and it is imperative that response teams effectively communicate information and coordinate actions among and between themselves. This section of your plan should contain:

- how communications and coordination will occur, by whom, when and how frequently
- the process that will be used to maintain effective communications and a coordinated response throughout the response effort.

More detailed guidance on communications is provided in section 7.

Managing issues and actions

Managing issues and actions during an incident is critical. An *Issues tracker* should be used by the Response Team to identify, prioritise and assign issues requiring action or resolution. Team members are expected to develop strategies and action plans to address assigned issues, and will be expected to report back on status to Response Team.

Note: an issues tracker template is available at www.faithassociates.co.uk/im to help you do this.

An *Action tracker* should be used to capture specific actions that are identified during Response Team meetings for assignment. This should be updated to capture status and completion of the actions, as the assigned team member reports to the team.

Note: an action tracker template is available at www.faithassociates.co.uk/im to help you do this.

Response team resources

Your plan should include details of the available team resources, including specialised expertise, teams or outside support, as well as physical resources and tools available. Resources should include the primary and alternate locations for Response Team meetings, technical and technological capabilities and communications availability. On-site resources and equipment for the Response Team should also be considered such as the following:

- hard-line and mobile telephones
- speakerphone capabilities
- audio/video capabilities, including projection/playback equipment
- television with cable connection
- computer(s) linked to external internet
- facsimile machine(s)
- copy machine(s)
- printer(s)
- audio/video recorder(s)
- back-up power supply
- battery supported radio(s)
- satellite telephone(s)
- white board(s)/black board(s)
- standard office supplies.

5. Response Plan

To manage the response to incidents should you now need to work up your **Response Plan** which should include the following key activities:

- notification and reporting
- concept of operations including communications and coordination
- plan maintenance
- training and exercising
- post-incident reviews.

Notification and reporting

Incidents and potential crises should be reported quickly with the Response Team put in place as needed so that resources and guidance can be provided in a timely way. Your organisation needs to define how a potential crisis or incident is reported and who is notified. A key objective of the initial reporting and notification process is to prevent incidents from escalating into a crisis for you. All incidents that meet the following criteria should be reported:

- an organisation-related death or serious injury of a staff member, service user, congregation member, contractor or visitor, or death of other person(s) caused by or attributed to any facility or resource of the organisation
- a building evacuation or quarantine resulting from an actual incident or threat (including due to contagious outbreaks)
- regional events that may impact the organisation's site(s), staff, congregation members, service users or local community
- potential service interruption expected to last for more than 24 hours
- an incident receiving significant adverse media attention
- breaking local or national regulatory requirements that the organisation is signed up to; either voluntary or a statutory requirement
- an inspection of premises expected to result in a fine or negative exposure
- unplanned investigations, premises inspections, local contagious health concerns etc
- a fire, explosion, hazardous material spill or release with the potential to adversely impact the local environment.

When reporting an incident or crisis an *Incident status report* should be completed that includes:

- the nature and severity of the event
- any response efforts underway
- the help needed.

Note: an Incident Status Report template is available at www.faithassociates.co.uk/im to help you do this.

What information should you attempt to provide?

Be prepared to provide as much information as you can, including:

- What happened?
- When did it happen? Where?
- Have there been any fatalities? Is anyone injured? Who are they?
- Are the injured being cared for?
- Have families been notified?

- Is anyone still in danger or in need of assistance?
- Is there damage to the organisations or local property?
- Is the crisis confined to our property or is the local community impacted?
- Have local authorities (police, fire, rescue) been contacted? Are they on-site?
- Is there potential for more damage?
- Is any hazardous material involved? Any release to the environment?
- Are news media on the scene? Who are they?

IMPORTANT: Do not wait until all of the information is available before reporting an actual or potential incident. If in doubt, make an incident report. If all of the information is not available immediately, further updates can be provided in the following hours and days.

You should consider whether to have an emergency number that staff, congregation members, service users, members of the local community and the emergency services can use. Many will already have nominated duty managers who pass a mobile phone between each other to an agreed schedule. The benefits of such an approach are:

- quickly escalate incidents to establish a Response Team as needed
- early identification of requests for additional resources and help
- inform key organisation staff as agreed in plans
- provide the Incident Status Report form to ensure consistent understanding of the known facts resulting in a timely and consistent report.

Concept of Operations

Your Response Plan should include a *Concept of Operations* (see section 4) that defines the process for what will happen. This should include guidelines around what can be done and the resources available. It should also include the level at which other help should be called on to provide additional support.

The concept of operations should also address the following practicalities:

- team structure
- activation
- communications and coordination
- open issues and actions status tracking
- response team resources.

Plan maintenance

Here you should include details of the process and anticipated timelines to ensure the planning documents are maintained and always up-to-date. The following are some general guidelines to consider:

- critical plan changes as the result of new guidance, new team members, or changing responsibilities/priorities should be implemented as soon as possible, or at least quarterly
- planning materials should be reviewed and updated after a practice or exercise activity
- changes should reflect lessons learned
- a complete document review and update should be completed annually.

Training and exercising

Your plan should define training and exercising activities (see section 6) to maintain a level of readiness and well trained and practiced Response Team. Here are some guidelines:

- all response team members should be trained initially and then periodically (at least annually) on the Response Plan, procedures and protocols. Refresher training should be scheduled periodically (eg quarterly), and can be combined with other activities or pre-planned meetings. When a new Response Team member is appointed, that individual should be trained on the existing plan as soon as possible
- the plan should be checked through an ongoing activities such as scenario-based table top discussion periodically (eg twice yearly) and a practical drill or exercise approximately every 12-18 months.

Incident close down and post-incident reviews

After an incident ensure there is a review of what happened. As part of the close down process in your plan, a review process and protocols should be defined. A post-incident review should be conducted every time your Response Team is activated and they have completed their response. This will provide an opportunity to review response procedures, identify areas for improvement and capture lessons learned.

6. Training and exercises

Exercising is an important step in assuring that all incident management preparedness elements within your organisation are aligned and well integrated. Building a response capability is more than just developing a plan; it is also about training and giving Response Team members an opportunity to practice implementing plan components.

Exercising gives your Response Teams an opportunity to validate the concepts, processes and protocols in their plans under hypothetical scenarios. Local government and Police representatives should be able to provide you with the opportunity to undertake a range of exercises. These types of activities normally will fall into one of the following:

- table-top exercises - facilitated scenario-based discussions that allow participants to work through realistic crisis situations, define or validate crisis management policy, and validate the organisation's incident management and response plans
- functional exercises - scenario-based exercise activities lasting four to six hours where participants are afforded the opportunity to demonstrate individual and team crisis management capabilities by reacting and taking actions based on a simulated crisis or emergency situation. Rather than simply discussing what the Response Team would do under the scenario (as in a Table-top exercise), the Response Team actually carries out their decision-making, response actions and communications process in real-time in a fast-paced, pressured environment
- full-scale exercises - scenario-based exercise that would involve your Response Team participating in a comprehensive validation of the crisis management and response capabilities of a local or regional area. Participants are afforded the opportunity to demonstrate individual, team, and organisational incident management capabilities and to show how linkages between the various different organisations and local services work.

Your organisation should look to plan and/or participate in at least one exercise activity every 12-18 months. It is recommended that when starting a training programme, Response Teams begin with a table-top exercise and then move on to a functional exercise. Full-scale exercises are more likely to be organised by local government or emergency services that your organisation will be invited to participate in.

7. Communications

Develop messages and making the initial communication

In most cases, you will need to develop a simple set of messages in response to an incident and develop communications for each of your key stakeholder groups; which includes appointing an appropriate spokesperson(s) to handle all media contacts. Communications today – where nearly every incident or issue can be broadcast worldwide in an instant – requires that you respond quickly. In these cases, a general statement that is non-committal regarding the facts, but expresses the organisation's concern is adequate eg

> *"We are working to address the situation, as well as to get an understanding of the facts. We will be back to speak with you as soon as possible."*

Define key groups to communicate with and plan how to do this

Beyond this initial statement and when developing a strategy for communications, ensure it is identifying a list of relevant key groups, defining their likely and relevant concerns and questions related to the situation, and then developing a communications plan to respond appropriately to the situation, while protecting your organisation. Here is a list of potential key groups to consider:

- staff
- congregation members
- service users
- local community
- other local faith institutions
- local emergency services – police and health
- local government including key contacts and politicians
- press and wider media
- board of trustees.

Communication during the management of the incident

As events unfold and as additional information becomes available, your organisation may want to communicate further. Communications efforts will need to evolve from a simple holding statement to messages and materials that better define:

- what happened
- how your organisation is responding
- what your organisation is doing to mitigate the crisis, including the protection of staff and the community
- how the organisation will continue to meet congregation and service user demands
- what the organisation is doing to prevent a similar situation in the future.

Here are some examples of key messages that may help you develop them for your organisation.

> *"Following our normal processes, we are closely monitoring the situation to manage its potential impacts on the personal health and safety of our staff, congregation, service users and local community."*

> *"We have a number of contingency plans and are in the process of implementing them."*

“We are committed to protecting the health and safety of our staff, congregation, service users and local community. Their personal health and safety is a top priority.”

“We are prepared and ready to support all of our congregation members and service users.”

“We continue to monitor the situation and will continue to keep you updated as needed.”

“We are working closely with local authorities - fire, police and emergency medical services - to protect and help our staff and the local community.”

“We are conducting an internal investigation to understand why this happened and more importantly so we can avoid a similar incident in the future.”

Address: Communication House
26 York Street
London W1U 6PZ

Telephone: + 44 (0) 845 273 3903

Email: info@faithassociates.co.uk

Web: www.faithassociates.co.uk