CPNI
Centre for the Protection of National Infrastructure

SECURITY-MINDED COMMUNICATIONS

Guidance for **Religious Establishments**

HM Government

Overview

Religious establishments across the UK are crucial components of society; they offer spiritual guidance, support to the vulnerable and a place for the community to come together. The very spirit of religious venues and events make them open and welcoming. However, this spirit and the beliefs that these venues and events represent make them attractive targets for people seeking to undertake criminal acts.

Religious groups regularly publish detailed information about their venues and events which, whilst useful for their congregation and community, can also be useful for another audience – those wishing to undertake a hostile act against their venue, event or people. These acts could range from petty criminality, such as theft, to ideologically, religiously, or politically motivated acts, like terrorism.

This guidance document provides information on the concept of Security-Minded Communications, which should be considered when publishing information for the public. The guidance can be applied at any time but is particularly relevant as you plan events following COVID-19 lockdowns which have prevented physical gatherings.

This guidance focuses on two main areas of Security-Minded Communications:

1) Ensuring that those with malicious intent are not unintentionally gifted information that they would find useful;

2) Showing how to deter these individuals using deterrence communications.

This guidance is important for all those who have contact with the public; the more interaction a member of clergy, staff or volunteer has with the public, the more opportunity they have to inadvertently provide information that would be useful to a hostile. However, these same people are also in an ideal position to deter those who wish to undertake hostile acts. It is therefore vital that all those involved in the running of religious establishments are aware of Security-minded Communications and wider security-mindedness. The Action Counters Terrorism (ACT) e-learning is a great foundation course that could be used as part of your mandatory induction for anyone involved in the running of your venue or event.

Summary
This document supplements existing Security-Minded Communications guidance and provides tailored guidance for religious establishments in the UK as to how they can use their communications channels to deny and deter hostiles from undertaking hostile acts against their venue or event.

Background

The Centre for the Protection of National Infrastructure (CPNI) defines a hostile as 'a person who wants to attack or disrupt an organisation for profit or to make a political or ideological point'. Research shows that there are three stages in a hostile's attack planning: target identification; detailed planning; and confirmation. A key part of the first two stages is hostile reconnaissance. CPNI defines hostile reconnaissance as 'purposeful observation with the intention of collecting information to inform the planning of a hostile act against a specific target'.

A hostile does not necessarily have to physically visit a site to obtain the information they require. They can use the internet to gather useful and current information from credible sources. Your communications can provide a potentially very effective layer of protective security, at little or no additional cost. By adopting a Security-Minded approach to communications and online content it is possible to deny the hostile the valuable information they require in their planning and deter them from undertaking their hostile act at your site.

This isn't a complicated process - small changes to noticeboards, social media posts, leaflets and posters can make a big difference to the security of your organisation, venue or event.

Denying hostiles information

What would a hostile want to know about a potential target site?

A hostile will be looking to obtain information that helps them to select a target, choose an attack time and understand what method of attack is likely to be most successful and fits with their motivation.

They will be looking for information on the protective security measures at the site and will be seeking to understand where there are vulnerabilities in those measures.

How would a hostile obtain that information?

A hostile will undertake hostile reconnaissance online as well as in person to inform their decision-making.

They may also seek to gain information from current or former members of staff, contractors or volunteers.

What can be done to deny a hostile this information?

When creating website content, social media posts, service handouts or any other communications (physical or online), consider the follow points:

- How much detail do **I need to** communicate?
- How can I ensure I provide information **without giving away details** that would be potentially useful to a hostile?
- How can I use this opportunity to **seed** messages that would deter a hostile?
- If I need to publish details, how can **I counter** any vulnerability created by promoting the protective security measures that are in place?

Denying hostiles information

Practical tips for religious establishments – denying hostiles information

You could consider the use of mailing lists, closed social media groups or group management software to ensure that you have control over who receives the most detailed information about your events and services. Less detailed information could be published more publicly with the option for people to request more details.

Consider whether you need to tell people exactly how many places are available at an event. If you advertise that there are 'only 100 places' and then subsequently those places are all taken, this tells a hostile how many people they can expect to be at their target.

If your place of worship is popular with the public for visits, consider the amount of detail you provide on maps of the site. Only show public areas on the map and limit the amount of detail you give in terms of dimensions and distances. Consider if you still need to publish a virtual tour and if you think it remains necessary, follow our other guidance on this.

Avoid providing detailed and direct contact details for people which may help a hostile undertake a 'spear phishing' attack. When arranging events use organisation email addresses, central telephone numbers and the main venue address rather than personal contact details. Alert your staff and volunteers to the existence of hostile reconnaissance and ensure they know how to report anything they see that they think is out of the ordinary.

Look through the information that you have already put in the public domain, or you are about to and check you are not accidentally gifting information of use to a hostile.

Using communications to deter hostiles

CPNI research shows how important it is to ensure that venues and events promote the security measures they have in place to deter those seeking to undertake hostile reconnaissance or malicious acts. The research also shows that members of the public want to hear more about what is being done to keep them safe. Places of worship are unique in their context and careful thought should be given as to what types of messages are used to ensure that they reassure rather than worry regular site users. This might include using phrases such as "looking for things that are out of the ordinary" rather than "suspicious" or advising that you want to "keep the site open and secure" rather than "stop criminals and terrorists".

Religious festivals and events

When considering religious festivals and events, it is important to recognise the importance of applying a Security-Minded Communications approach to your plans. Consider the additional vulnerabilities of large-scale events in more open locations, including our guidance on protecting queues of people, and consider how you can reassure people that you are taking security seriously, but in a way that is sensitive to the context.

It's never too early to begin to adopt Security-Minded Communications. Once implemented it should be applied continuously. This might include considering post-event/festival comments or reviews. For example, if someone comments on your social media channels saying how good it was to see so many people at the event, a simple reply acknowledging this and thanking the large number of staff and volunteers for ensuring the event was successful, safe and secure or thanking the local police, business or community group for their partnership at the event would be a 'security minded' response.

Using communications to deter hostiles

Practical tips for religious establishments – deterring hostiles

Use your community bulletin boards to display posters promoting community vigilance. Make it clear who concerns should be reported to (for example to call 999, 101, call the Anti-Terrorist Hotline in confidence on 0800 789 321 or report online at gov.uk/ACT) and give people confidence that reports will be acted upon.

Establish and publicise the partnerships you have with other organisations. This could be through a social media post of the local police or PSCO visiting your place or worship, highlighting a network of good communication with local community groups or even something as simple as publicising that you communicate with your local coffee shop.

Ensure that pictures of staff and volunteers show them wearing something that makes them stand out as staff/volunteers such as a lanyard, pass or uniform. Make sure images don't provide helpful detail for a hostile either by blurring out those details or turning the pass over.

Be proactive in answering public comments or questions that are posted to your social media pages or for larger venues, review sites. This shows a hostile that your venue or event is alert to people seeking information or posting about them.

Avoid posting images that reveal the extent of your security features. This might mean changing photos that show the type of alarm you have installed, the doors that are difficult to secure or the placement of any CCTV you may have.

Where possible be ambiguous about when your venue is occupied. Social media posts outside of normal office hours and outside the hours that the venue is occupied can give the impression that it is busier than perhaps it is and could prevent a hostile from being able to establish when would be a good time to undertake their act.

Consider using your COVID-19 safety messaging as an opportunity to weave in security messaging. We have some further guidance that can help with how to do this.

Further guidance and advice

Your local Counter Terrorism Security Advisors will be able to provide further advice on police partnerships and appropriate protective security measures. There is also a wealth of guidance available on the CPNI website that you might also find useful when considering what measures you can take to help keep your place or worship and religious events secure. The guidance we recommend is:

Understanding Hostile Reconnaissance and countering the threat

Disrupting Hostile Reconnaissance

NaCTSO Crowded Places Guidance

Action Counters Terrorism

Security-Minded Communications- Virtual Tours Guidance

Staying Safe During COVID-19

Should you have any questions or require further assistance please contact us through the CPNI website.

Disclaimer

The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it. This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, CPNI accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at www.cpni.gov.uk.

Freedom of Information Act (FOIA): This information is supplied in confidence to the named reader and may not be disclosed further without prior approval from CPNI. This information is exempt from disclosure under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.