

Martyn's Law — What Will You Actually Say?

Of the four public protection procedures in the Act, communication is the one I think gets the least attention.

The other procedures are easier to picture. Doors, routes, safe spaces, locks. You can walk them.

Communication is harder to see. But without it, none of the others start.

That's what I want to look at here: what you'll say, who will say it, and how it will reach people.

I've been thinking about why that matters so much to me.

In my first blog, I talked about my role leading organisational learning in Counter Terrorism Policing. Part of that role was understanding the points of failure. Through strategic debriefs post incidents, our challenge was to understand and review what had happened operationally. What worked. What didn't. And why.

Sadly, communication was often a core component of where failure was identified. It could be anywhere in the chain: how calls for help were locally received, understood and prioritised, how information moved between the people on the ground and the people making decisions, and how effectively agencies engaged with each other once the response was under way.

The emergency services may operate at a different level to a shop, a hotel or a college. But the principle holds. In an unfolding incident, communication shapes how people respond. For premises, that means two things: how you communicate within your own location, and making sure the right information reaches the emergency services so they can respond effectively.

The Manchester Arena Inquiry is a reminder of how much this matters. Communication featured in its findings, both inside the venue and across the wider emergency response. Information didn't always reach the people who needed it, when they needed it. The Chairman was clear that the purpose of examining what went wrong was to learn from it and prevent it happening again, not to apportion blame. That's the spirit in which I raise it here.

What the legislation asks for

The Act describes this procedure as providing information to individuals on the premises or at the event (section 5(3)(d)). The statutory guidance uses the term communication. It describes the purpose as alerting people to danger as quickly as possible and giving them instructions where it's safe to do so, and it makes the point that effective communication is what enables the other procedures to be started quickly (paragraphs 7.46 and 7.47).

That feels right to me. You can have a well-designed plan, but if nobody hears the instruction, or hears the wrong one, it won't work.

The guidance then asks the responsible person to think through some practical questions (paragraph 7.48). What information needs to be given, and might the public need something different to staff? Who shares it, and how does it flow between staff and the people making decisions? How will you get it out quickly, in a way that works for your premises? And how do you embed all of that before you ever need it, through documenting, briefing and testing?

You won't always know what you're dealing with

Looking back at many of the attacks in the UK in recent years, one thing stands out to me. In the first moments, it may not be clear that it's a terrorist attack at all.

What staff actually see is people running, someone injured, a traffic accident, noise, chaos. Nothing arrives with a label on it. So decisions have to be made on the best information available at the time.

The legislation reflects that. The Act's procedures are for when there is reason to suspect an act of terrorism is occurring, or is about to occur (section 5(3)). Not when it's confirmed. The guidance says the exact nature of an attack may not be immediately obvious, and that quick action is likely to be the most effective way of reducing harm (paragraph 7.18).

It even gives an example of a Standard Tier shop where staff hear activity outside and see panicked people rushing towards the doors. They don't know exactly what's happening, but the duty manager brings people inside and locks down (see the examples following paragraph 7.19).

During the London Bridge and Borough Market attack on 3 June 2017, staff at Arthur Hooper's restaurant and wine bar realised something was happening outside and brought people inside to shelter. Sergio Fariña, who ran the restaurant, was trying to secure the entrance when one of the attackers tried to get in. He held him off and prevented him getting inside. The CCTV of that moment is something I use in my presentations.

I have no doubt that his actions, and those of his staff, saved lives.

The example brings together rapid decision-making, securing the premises and helping people shelter.

In an interview with [El País](#) published on 5 August 2017, Fariña described how loud music and kitchen staff working downstairs made it difficult to alert everyone quickly.

For me, this brings the communication question into sharp focus. Can you reach the people working in every part of your premises? Will they understand the instruction, and can they help others act on it? It's an example worth keeping in mind when you test your own arrangements.

How it reaches people

There's no single right way to communicate in an incident. The guidance recognises it can take many forms, from verbal communication and briefings to signage, posters and audio broadcasts (paragraph 7.47), and that the right method depends on the premises (paragraph 7.48).

At its simplest, it's a member of staff shouting a clear instruction. In a small café or shop, loud, clear verbal commands may be exactly the right approach, and the guidance says so.

Larger or more complex premises may need a combination of methods. A PA or tannoy system. Loud hailers or megaphones. Closed radio systems, and in some venues headsets, so staff can talk to each other and to whoever is making decisions. Alarms. Digital screens. And, increasingly, apps.

Apps deserve a particular mention, because they're where a lot of organisations are now looking.

Used well, an app can do things a PA system can't. Depending on its capabilities and coverage, an app can send alerts across a large site and may allow staff to acknowledge receipt. Between

neighbouring premises, a shared channel can help too. The guidance's own shopping centre example has duty managers establishing a real-time communications channel with each other (see the example following paragraph 7.63).

But an app is one part of the answer, not the whole of it. It depends on people having their phones on them, charged, with signal, and actually looking at them. In an attack, people may be running, hiding, or silencing their phones to stay hidden. Most members of the public on site won't have your app at all. So I'd see it as something that strengthens a communication procedure, not something that replaces a clear voice, a PA system or a radio.

As with any technology in this space, do your due diligence. Understand exactly what it does, test it in the conditions you'd actually use it in, and make sure your people know how to use it before the day they need it.

Whatever you use, the same questions apply. Will it work on a busy, noisy day? Will it reach people wherever they are, including those who can't hear an announcement, don't speak English as a first language, or may need more support to act on it? What happens if it fails, or if everyone tries to use it at once?

And it isn't only about what you say to the public. Staff need to talk to each other, and information needs to reach the person who can make a decision. That's often the first communication that has to happen, and the one most easily overlooked.

How you say it matters too. The guidance asks for information that is simple, clear and specific to the action required (paragraph 7.48). In an incident, that means short, calm, direct instructions: move away from the windows, follow me to the back of the building. Not a long explanation of what might be happening.

Making use of what's already out there

ProtectUK has good, free advice that sits well alongside the statutory guidance. Two pieces I'd point any business towards are Run Hide Tell and Guide Shelter Report. They sound similar, but they do different jobs.

Run Hide Tell is Counter Terrorism Policing's advice for members of the public caught up in a firearms or weapons attack: run if you can, hide if you can't, and tell the police by calling 999 when it's safe to do so.

Guide Shelter Report is NaCTSO's business-focused version, launched earlier this year. It was developed on the back of feedback from businesses that Run Hide Tell didn't account for their staff's duty of care towards the people around them. It complements Run Hide Tell rather than replacing it: guide people away from danger, shelter them to keep them safe, report to police by calling 999.

What struck me reading it is how closely it lines up with the Act. NaCTSO's own material maps Guide and Shelter directly onto the public protection procedures the Act requires. And communication runs through all of it.

If a member of staff is expected to guide people, what will they actually say? If people need to shelter, how will staff tell them where to go? Who reports to police, and what will they tell them? The guidance asks that last question directly: who will alert the emergency services, and what information they should give (paragraph 7.28). The ETHANE mnemonic in the Guide Shelter

Report material is a helpful structure for that call. Getting it right shapes what the emergency services send, and where.

Posters and briefings have their place. But NaCTSO makes the point in its own Guide Shelter Report guidance that telling staff about the principles isn't enough; the arrangements have to sit behind them. The statutory guidance says something similar: staff need to understand the procedures and their own role in them, with instruction or training as needed (paragraph 7.28).

Bigger sites, bigger questions

For larger and more complex premises, the guidance asks more (paragraph 7.49). Will the message actually reach people wherever they are on site? Are the instructions for each procedure clearly different, so people know exactly what's being asked of them? Could the communication procedure be used on its own, for example to raise awareness of suspicious activity, without triggering anything else?

Those considerations aren't tied to a tier. They apply to larger and more complex premises, whichever tier they sit in.

For some Standard Tier premises, the guidance goes further again. Places of worship and education settings, other than higher education, stay in the Standard Tier even when 800 or more people could be present. For those premises, and for larger or more complex Standard Tier premises generally, it may be appropriate to consider the additional considerations written for Enhanced Tier premises and qualifying events (paragraphs 7.30 and 7.31).

When I think back to the college estate I wrote about recently... Multiple campuses. Teaching blocks, sports halls, accommodation. One message won't reach all of those people in the same way, and it probably shouldn't say the same thing either.

Writing it down

Standard Tier premises have no legal requirement to document their procedures. But the guidance says the responsible person should, so that procedures can be understood and communicated to staff, and because it may be difficult to demonstrate compliance to the SIA without it (paragraph 7.32). It needn't be complicated. A briefing, quick reference guide or prompt card can help staff understand their roles and the actions required (paragraph 7.58).

The best communication procedure in the world won't help anyone if it lives in a folder in the manager's office.

What will you actually say?

In my first blog, I said that if I were sitting with a business today, I'd ask whether their people would know what to do if something happened tomorrow.

I'd add a second question now. Would they know what to say?

If the honest answer is "we'd work it out on the day", that's the place to start. Decide the words now. Decide who says them, and how. Then practise them, so that people can act confidently and adapt as the situation changes.

Danielle Grant

Director of Counter Terrorism & Protective Security

Global Consortium Group (GCG)

Danni Grant is Director of Counter Terrorism and Protective Security at Global Consortium Group and a former senior national leader in UK Counter Terrorism Policing. She held national responsibility within Protect and Prepare, leading work across organisational learning, training and exercising, and working with government, policing and partners to strengthen preparedness for terrorist attacks.

Today, she advises organisations on Martyn's Law, protective security and practical approaches to preparedness, response and recovery.