

# Security On Your Side Implementation Guide

## SECURITY ON YOUR SIDE

Areas like this are filled with  
security measures.

Some you can see,  
some you can't.

#SecurityOnYourSide



## In this pack...

<b>Page 3</b>	Campaign Rationale
<b>Page 4</b>	So... What is Security On Your Side (SOYS)?
<b>Page 5</b>	Pre-Campaign Activities
<b>Page 6</b>	Deploying your assets
<b>Page 7</b>	Asset Siting Guide
<b>Page 8, 9 &amp; 10</b>	Signposting Your Security Measures
<b>Page 11</b>	Social Media Guidance
<b>Page 12</b>	Social Media Examples
<b>Page 13</b>	FAQ's
<b>Page 14</b>	Post Campaign Activities
<b>Page 15</b>	SOYS Assets



## If a hostile believes your venue is secure, they are less likely to progress with their attack planning.

One of the most significant threats facing the UK are vehicles as a weapon (VAW) - this is where a hostile deliberately drives a vehicle at an individual or crowd to cause harm. Across the UK in venues and public spaces like yours, Hostile Vehicle Mitigation (HVM) barriers have been installed. As some of these measures are increasingly designed into normal street furniture (i.e. benches, bins, planters) it was realised that they may lose their visual deterrence. Similarly, more traditional HVM such as bollards and barriers are also becoming a regular feature of today's street scape.

**Our extensive research has shown that the planning process that a hostile will go through, and the characteristics they show, present opportunities that can be used to keep you safe.**

Using communications to amplify security measures, you can deter hostiles from undertaking illegal activity including crime, illegal protest, terrorism and threats from other states. These types of communications have been extensively tested and we know that they can be perceived as reassuring by the public. This is known as **Security Minded Communications (SMC)**.

NPSA sought to create a campaign, that highlights and increases the deterrent effect of security measures at your venue/organisation or event, such as HVM and other features (CCTV, Security Patrols etc), and that indicates the presence of other security assets which aren't immediately obvious...

**'Some you can see, Some you can't...'**

Extensive testing was conducted at the design evaluation stage, using key target audience perspectives to determine how the campaign was received, with a particular focus on the extent to which the public felt reassured by the campaign's messages. It was after this testing, and in combination with the results from trials by experienced 'proxy hostiles' conducting hostile reconnaissance, that 'Security on Your Side' was born..

**Security-Minded Communications (SMC):** is an approach developed by the NPSA. It has been informed by an extensive research programme and can help to equip organisations, venues and events with the ability to use communications as part of your protective security measures. It is designed to disrupt hostiles during the reconnaissance stage of their planning.

**Hostiles:** NPSA defines hostiles as individuals who want to attack or disrupt an organisation for profit, or to make a political or ideological point. Hostiles can be terrorists, organised criminals, those using illegal protest activity or threats from other states.



# So...What is 'Security on your Side'?

**Security On Your Side (SOYS)** is a newly developed Security Minded Communications (SMC) campaign designed with the everyday site user in mind. It's a toolkit of communication assets, layered across a range of communication channels, that amplifies the Hostile Vehicle Mitigations (HVM) and other security measures that could be in place at your venue, organisation or event.

Informed by our extensive research and using tried and tested techniques from our SMC approach, the **Security on Your Side** campaign can enhance your customer service by making your customers and visitors feel safe, whilst creating the opportunity to exploit and exacerbate a hostile's feelings of paranoia and anxiety that they may be caught or disrupted during their attack planning. This campaign has two objectives:

- **To reassure the everyday site user.**
- **To deter those with hostile intent.**

This 'Implementation Guide' is designed to assist venues, organisations and events to get the most out of using the 'Security On Your Side' campaign assets, and ensure these objectives are met.



## Securing Support and buy-in and Stakeholder Engagement

To host the Security on your Side campaign at your venue/organisation/event it will require a coordinated effort from all stakeholders, therefore having their support is key. Initially, you should consider all the groups within your organisation that have a vested interest in a security campaign. Consider who needs to be involved to ensure all the objectives are met:

- **Senior Management Team** – ultimately, buy-in and support from the organisational decision makers is key,
- **Communications team** – website and social media campaign elements and schedules, public image/reputational issues and ‘branding’.
- **Briefing of Security Officers** – the public facing security teams are a key message delivery mechanism, buy-in and campaign awareness is critical to ensure they know how to respond to reports and signpost reporting routes.
- **HR & Training** – awareness and wider education of the campaign and to reinforce the reporting structures.
- **Service desk or helpline personnel** – to ensure awareness of reporting structures and they know how to respond to reports.
- **Security incident management** – alive to the potential of increased reporting during a campaign.
- **Legal** – to ensure report information is treated appropriately, processes adhere to necessity and proportionality rules, and relevant legislation is understood.

To help with gaining their support and buy-in you should be prepared by considering the following:

- What are the overarching objectives – why are you running the campaign for your site?
- What does success look like – have you got the right benchmarks for evaluation in place? See Page 14 of this guide.
- Do staff support the security campaigns and see their value? Do they understand the concept of SMC. Have they been trained to support a campaign or how to spot suspicious behaviour and hostile reconnaissance, are they SCaN trained?
- Are there any individuals within the business who are enthusiastic about security who can be ‘champions’ or ‘campaign ambassadors’?
- Can you provide a rationale and justification for the campaign if you are challenged by colleagues?

### Crucial Senior Team Buy-In

Delivering the message to your Senior Management Team and a good partnership with security lead & comms are essential. The NPSA Extranet has some useful tools to assist in selling the benefits of a SMC approach at your organisation/venue/event:

[https://extranet.npsa.gov.uk/system/files/documents/npsa-how-to-guide-security-minded\\_comms.pdf](https://extranet.npsa.gov.uk/system/files/documents/npsa-how-to-guide-security-minded_comms.pdf)

<https://extranet.npsa.gov.uk/security-minded-communications-videos>



**Our extensive evaluation and piloting has shown that asset siting is key for Security On your Side to have the impact required to be successful in its objectives (reassure everyday site users/deter those with hostile intent). We recommend using a multi layered approach to your SOYS campaign:**

## **IMPORTANT NOTE: Choosing your assets**

**When choosing your downloadable assets, you must ensure they properly reflect your organisation/venue/event and that the security measures that feature on the assets are present at your site. This is important to the integrity of the message and the legitimacy of the deterrence effect.**

## **Principles of good communication: Reach & Frequency**

For communications to cut through to their intended audience, particularly in a crowded environment follow the principle that the more people that see your communications the better the return on the investment. Providing multiple opportunities to see the communication assets will help the message land with the intended audience.

## **Layering**

Use all available communications channels available to your site. For the public, this means leveraging posters, digital communications (website and social media), audio, PR and direct contact from staff who can act as a good communications conduit and force multiplier.

## **Siting**

Be sure to target areas of high footfall to optimise reach and consider your site user's journey.

Balance with areas where visitors have longer dwell times and are therefore a captive audience: body & bag screening, queues, food and drink concessions, toilets are common examples. Further information on siting is provided on the next page.

## **Sizing**

Ensure the assets are large enough to be noticed and read. The assets provide a good amount of detail on them, consider the clarity of this detail when they are displayed.

## **Formats**

With posters use a combination of mobile and fixed sites and static and digital versions to give flexibility and placement throughout the full site user journey. The next page highlights the areas where there are opportunities for people to see the assets.





## Consider the Site Users' Journey

Key to delivering the 'Security on Your Side' message is placing the assets at multiple locations throughout the site user' journey.

### Pre-Visit Online Site Research

Most site users will research your organisation/venue/event online before visiting. Consider SOYS in your security messaging so there is a greater chance of it being seen even before they arrive.

Using the digital images around your site's security pages is a good way of seeding familiarity with the messaging and can be the start of a site user noticing the assets on their journey through your venue.

### Transport Connections/Hubs

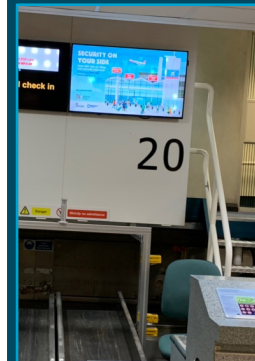
Coordinating with local transport hubs to capture site users on their journey can be advantageous. If it is within your site's gift, consider:



- Bus/Tram stops
- Car parks
- Taxi ranks
- Foot routes from transport hub to site
- On board shuttle buses/trams

### Security Search Areas / Dwell Areas

Areas where site users will dwell offers more opportunity for messaging to be noticed:



- Check-in
- Foyers
- Waiting areas
- Reception Desks
- Seating areas/Benches
- Information displays
- Toilets/Restrooms

### Queueing Areas

Queue lines are a key area that has a captive audience. Using A-frames or queue barrier sign holders are a good way of capitalising on the site user's time in the queue.

Consider:

- Security queues
- Bag drop queues
- Transport queues
- Ticket/box office
- Customer service
- Entry / exit queues



### Partnership Engagement

Telling your site users that you engage with local law enforcement, businesses and transport hubs is a good way of showing collaboration and that you take your sites' security seriously.

If appropriate, use social media assets to tag local businesses and partners and encourage them to share the message via their social media channels. Law enforcement can be willing to share onwards messaging also. Consider SOYS assets at local business in the vicinity of your site.

### Social Media



Social Media is an important engagement tool for your site user. Consider using a layered approach to your campaign's communications strategy.

More on page 11.

### High Footfall Routes

The higher footfall route through your venue is a good strategic place to site communications:



- 'Fan-zones'
- From entry to destination (seat / office / platform / gate)
- Concourse
- Departures/Arrivals

### Food Outlets / Concession Stands

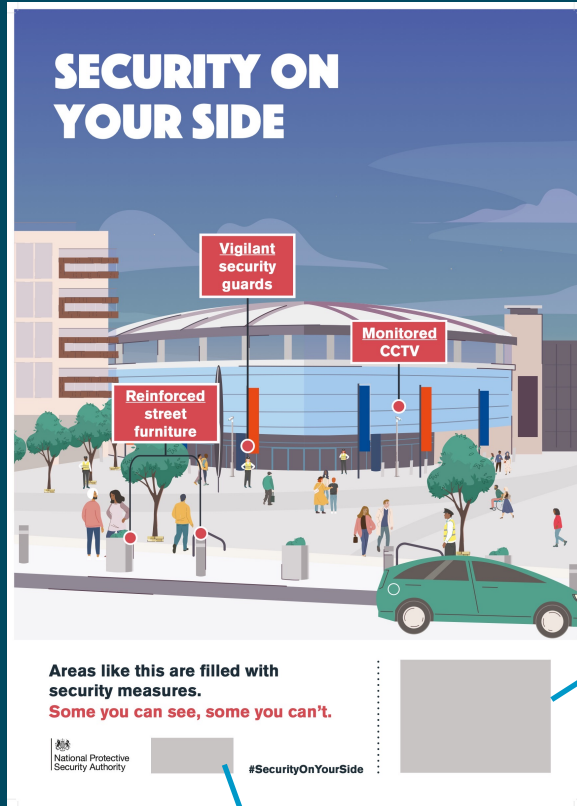
Using electronic displays that feature all around your venue is a great way to deliver repeat messaging:

- Bars/Kiosks
- Food Outlets
- Gift shops
- Stalls
- Merchandise



# Signposting Your Security Measures

Add your company logo next to NPSA to show collaboration. Use the larger editable area in the assets to signpost to your organisation/venue/event's home security page as a 'call to action'. Here are some examples of what you might include in the editable areas:



Your company logo here

Find what else we are doing to keep you safe by visiting:

[www.yourvenue/security](http://www.yourvenue/security)

If you see anything suspicious contact our security team on .....

Find out what Security is on your side by visiting:

[www.yourvenue/security](http://www.yourvenue/security)

If you see anything suspicious speak to one of our security team.

**Always dial 999 in an emergency.**

Find out more about how we have teamed up with the NPSA and local Police to keep you safe, visit:

[www.yourvenue/security](http://www.yourvenue/security)

**Always dial 999 in an emergency.**

We're committed to reducing all forms of crime and to do this we're using a range of security measures. While some of these measures are visible, we also have a lot going on behind the scenes.

Find out more by visiting:

[www.yourvenue/security](http://www.yourvenue/security)

**IMPORTANT:** Assets should not be implemented without this detail being added. Ensuring your site users know how they can report suspicious activity and a good organisational response is a key aspect of a good security campaign. Consider your reporting mechanisms, response times and feedback loop.





# Signposting Your Security Measures



Use the security pages on your venue/organisation/events website to amplify the SOYS security messaging. Examples of the type of messaging you could use:

We've teamed up with the **National Protective Security Authority** to enhance our security, help you feel safe and enjoy your time at our <<venue/organisation/event>>.

We're committed to reducing all forms of crime and to do this we're using a range of security measures. While some of these measures are visible, such as <<barriers, CCTV cameras, and our vigilant security staff,>> we also have a lot going on behind the scenes.

At our <<venue/organisation/event>> your safety and enjoyment are our top priority, so while it's not always obvious what we're doing to keep you safe, we wanted you to know there's always...

**SECURITY ON YOUR SIDE**

We have various security measures in place, some which you can see and some of which you can't. Rest assured that at this <<venue/organisation/event>> **there is always...**

**SECURITY ON YOUR SIDE**

We're delighted to announce our collaboration with the NPSA to enhance the security of our <<venue/organisation/event>>. We've implemented a range of security measures to keep you safe, while some of these may be visible there is also a lot going on behind the scenes.

**At <<venue/organisation/event>> there is always...**

**SECURITY ON YOUR SIDE**

# Signposting Your Security Measures

Talk about the security assets that feature at your venue within your security pages. If you have HVM, CCTV, SCaN trained staff or you know SERVATOR deploys at or around your site, consider using this content:

## SCaN

Our Staff have undergone specialist training to spot hostiles who are undertaking reconnaissance and know what to do about it.

See, Check and Notify (SCaN) is a specially designed program that educates staff throughout the company. It helps ensure that individuals or groups seeking to cause the public or an organisation harm are unable to get the information they need to plan their actions. SCaN can be the difference between a terrorist, or other criminal, seeing an organisation, venue or event as a potential target, or perceiving it as too difficult and abandoning their plans.

Find out more here: <https://www.npsa.gov.uk/see-check-and-notify-scan>

## Police Engagement/Deployments

The uniformed officer you can see, the plain clothed officer you can't, together with the specialist detection dog all may be part of a Project SERVATOR deployment.

Project SERVATOR is a policing tactic that aims to disrupt a range of criminal activity, including terrorism, while providing a reassuring presence for the public. It is deployed by policing teams nationwide and can happen regularly, anytime and anywhere. The teams can be made up of a range of highly visible assets, such as uniformed police officers, dogs and horses, armed officers and vehicle checkpoints. Others are less visible, such as plain clothes officers, and CCTV operators.

Project SERVATOR teams work with the community – businesses, partners and members of the public – to build a network of vigilance and encourage suspicious activity to be reported.

Find out more here: [counterterrorism.police.uk/servator](https://counterterrorism.police.uk/servator)

## HVM

At this venue we have specific features that have been designed to offer you protection from a vehicle as a weapon attack. These are known as Hostile Vehicle Mitigations.

You can learn more about how effective these are by visiting <https://www.youtube.com/watch?v=Y5betsX3LHo>

## CCTV

Our CCTV cameras are monitored 24/7 with a direct link to Police security control rooms and security guards on the ground who have practiced their response to various threats and know how to deal with them.



This section is designed to support the development of digital content for the Security on Your Side campaign. It contains Key Messages that should inform content development. Examples of how these key messages can be used are also included.

Venues can utilise the provided wording in its current form, or alternatively, use it as guidance to shape their own messages, in order to align with the tone and content requirements of their broader communications strategies.

## Key Messages

Venues should aim to include the sentiment of these messages in communications they produce in relation to the SOYS campaign:

- We use a range of security measures.
- Some you can see, some you can't.
- We are working with NPSA and other key partners to keep you safe.

**Note 1:** It may not be possible to apply all key messages to every piece of content produced.

**Note 2:** Avoid any wording that implies an attack is imminent.

**The next page provides some social media examples to guide you.**

## Social Media Posts

A good social media campaign will be coordinated across platforms during the campaign life cycle and compliment your security. Consider the Security Minded approach in all your public communications. Think about the timing and sequencing of posts, and multiple, coordinated messaging.

Talk about security successes, law enforcement partnerships (local Police contact, PCSO, CTSA, Project SERVATOR etc.) collaboration with other sites and transport hubs to show a network of vigilance that will resonate with the public and with hostiles.

**REMEMBER:** Be security minded in all your communications  
<https://www.npsa.gov.uk/security-minded-communications-guidance>



# Social Media Examples



## Example 1 – Focus on Measures

We thought you'd like to know that we're using a range of security measures to reduce crime and other harmful activities at our <<venue/organisation/event>>. Some of them you'll be able to see, like vehicle barriers, CCTV cameras and security staff, but there are lots of other measures that you may not notice.

It's not always obvious what we're doing to keep you safe, but we want to you know there's always...

SECURITY ON YOUR SIDE

#securityonyourside



## Example 2 – Focus on NPSA

We're delighted to announce our collaboration with the NPSA to enhance the safety of our <<venue/organisation/event>>. We've implemented a range of security measures to keep you safe from all forms of crime. While some of these may be visible there is also a lot going on behind the scenes.

It's not always obvious what we're doing to keep you safe, but we want to you know there's always...  
SECURITY ON YOUR SIDE



Areas like this are filled with security measures.



## Example 3 – Short version

It's not always obvious what we're doing to keep you safe, but we want to you know there's always...

SECURITY ON YOUR SIDE

#securityonyourside





These FAQs and their responses are designed to be used as a guide by venue staff who are questioned by the public about the SOYS campaign, and its intended purposes. These answers should only be given in direct response to questions, they do not need to be released proactively.

### What is the SOYS Campaign / what is it about.

The campaign is designed to make people more aware of the measures that venues use to keep their customers, guests, and staff safe. We hope the campaign makes people feel reassured.

### Who has been involved in developing the designs?

This has been led by the Government. We employed an external media agency to develop the designs. The designs have also been tested on the public in focus groups and in a pilot at sites across the UK.

### Is this about crime or terrorism?

Although this campaign has been developed as part of a review of counter-terrorism measures, the messages that indicate that security measures are in place are also applicable to crime.

### Is this campaign being launched in response to any particular incident?

No, the UK government continues to take proactive steps to protect people from crime and terrorism, this is just one of many steps we are taking to achieve this.

### If this campaign is deployed at this venue, does it mean you think this venue is at greater risk of attack?

No, not at all. We have no intelligence that indicates there is going to be an attack at this venue. This campaign is a proactive measure that is designed to reassure the public that their safety is a priority.

### Is there intelligence that a terrorist attack is planned?

Whilst we cannot comment on intelligence matters or specific threats, we know the UK faces a real and serious threat from terrorism. The current threat to the UK from international terrorism remains 'SUBSTANTIAL', meaning an attack is LIKELY.

### There are already too many security messages, why do we need these?

We will not be adding to the number of security announcements you hear at venues; this campaign will replace existing security messages.

### Do these posters stereotype particular groups?

We used illustrations rather than photography in the poster designs to avoid identifying particular groups. However, we need to make sure the public can identify the scenarios that are being illustrated in the campaign, so we wanted to use a range of individuals.

### What is the Government doing to meet the terrorist threats?

It would not be appropriate to describe the security measures that are in place as this information could be useful for those seeking to cause harm to others. However, the Government takes security very seriously and there are a range of measures in place to help reduce the likelihood of an attack, which are under constant review.

### Why are you launching a new campaign? Weren't the old ones effective?

Yes, they were effective. However, we are always seeking to evolve and improve our approach to security. This is just one example of how we do this.



## Evaluation and Review

### Evaluate your campaign

Consider your own End-of-phase evaluation at your site to measure the efficacy of SOYS within the context of your organisation. This can be a good tool to provide to the senior team for further engagement and buy-in for future campaigns.

Consider the following ways to measure success of the campaign:

- Social media engagement; Your comms team will be able to provide a social media engagement report to include impressions, reaction, reposts/shares, comments and clicks.
- Site Security Reporting: have the levels of suspicious reporting increased during the campaign? Clear reporting instructions on the assets are key here.

Consider the question: 'Is this campaign making a difference to the security of my site, venue?'. Using anecdotal information from contextual experts who have been present during the campaign such as:

- Front facing staff (Security/cleaners/reception staff/customer service staff)
- Security managers and other individuals who will receive reports
- Members of the target audience

Snap surveys and questionnaires of your site users is an important tool to measure reach and impact.

### Review and Refresh

Keeping on top of your assets' health is important to the integrity of the message and the deterrence effect therein. This includes keeping security messaging on your communication channels current and reporting channels/contact details up to date. Tired, neglected posters, out of date communications details and/or unanswered under-valued security reporting is detrimental to the security of your site and the impact of your deterrence messaging.

Regularly review and refresh your communication assets and campaign security procedures. Research shows that when you take your security seriously, deterrence messaging can disrupt hostile intent.



# Downloadable SOYS Assets



National Protective Security Authority

Bridge Scene

**SECURITY ON YOUR SIDE**

Plain clothed Police  
Reinforced street furniture  
Regular Police Patrols

Areas like this are filled with security measures.  
Some you can see, some you can't.

National Protective Security Authority #SecurityOnYourSide

Train Station Scene

**SECURITY ON YOUR SIDE**

Monitored CCTV  
Reinforced street furniture  
Plain clothed Police

Areas like this are filled with security measures.  
Some you can see, some you can't.

National Protective Security Authority #SecurityOnYourSide

Market Scene

**SECURITY ON YOUR SIDE**

Specialist Detection Dog  
Reinforced street furniture  
Monitored CCTV

Areas like this are filled with security measures.  
Some you can see, some you can't.

National Protective Security Authority #SecurityOnYourSide

High Street Scene

**SECURITY ON YOUR SIDE**

Reinforced street furniture  
Vigilant Security Officer  
Security trained shop worker  
Monitored CCTV

Areas like this are filled with security measures.  
Some you can see, some you can't.

National Protective Security Authority #SecurityOnYourSide

Stadium/Arena Scene 1

**SECURITY ON YOUR SIDE**

Reinforced street furniture  
Vigilant security guards  
Monitored CCTV

Areas like this are filled with security measures.  
Some you can see, some you can't.

National Protective Security Authority #SecurityOnYourSide

Stadium/Arena Scene 2

**SECURITY ON YOUR SIDE**

Reinforced street furniture  
Vigilant security guards  
Monitored CCTV

Areas like this are filled with security measures.  
Some you can see, some you can't.

National Protective Security Authority #SecurityOnYourSide

International Airport Scene

**SECURITY ON YOUR SIDE**

Monitored CCTV  
Specialist Detection Dog  
Reinforced street furniture

Areas like this are filled with security measures.  
Some you can see, some you can't.

National Protective Security Authority #SecurityOnYourSide

Regional Airport Scene

**SECURITY ON YOUR SIDE**

Reinforced barriers  
Police patrols  
Monitored CCTV

Areas like this are filled with security measures.  
Some you can see, some you can't.

National Protective Security Authority #SecurityOnYourSide

OFFICIAL

**NPSA would love to hear how you have deployed ‘Security On Your Side’ across your site & would welcome any feedback so that we can continue to develop this toolkit based on customer experiences.**

**Contact: [NPSA-Enquiries@NPSA.gov.uk](mailto:NPSA-Enquiries@NPSA.gov.uk)**

## Disclaimer

*This guide has been prepared by the National Protective Security Authority (NPSA) and is intended to guide the implementation of the security campaign ‘Security on Your Side’. This document is provided on an information basis only, and whilst NPSA has used all reasonable care in producing it, NPSA provides no warranty as to its accuracy or completeness.*

*It is important to emphasise that no security measures are proof against all threats. You remain entirely responsible for the security of your own sites and/or business, compliance with any applicable law and regulations and must use your own judgement as to whether and how to implement our recommendations.*

*To the fullest extent permitted by law, NPSA accepts no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using the implementation guide. This exclusion applies to all losses and damages whether arising in contract, tort, by statute or otherwise including where it is a result of negligence. NPSA separately and expressly excludes any liability for any special, indirect and/or consequential losses, including any loss of or damage to business, market share; reputation, profits or goodwill and/or costs of dealing with regulators and fines from regulators.*

© Crown Copyright 2023.

*You may use or reuse this content without prior permission but must adhere to and accept the terms of the Open Government Licence for public sector information. You must acknowledge NPSA as the source of the content and include a link to the Open Government Licence wherever possible. Authorisation to reproduce a third party’s copyright material must be obtained from the copyright holders concerned.*

