CEMEX UKNEWS

Zero harm for Life

Welcome to UK News 28th March 2018
your weekly update from around CEMEX UK

View UK News on: www.cemexuknews.co.uk
Follow us on twitter too: @CEMEX_UK

BEING THE BEST FOR FAMILIES

Weekly Health And Safety Message From Michel

Hopefully the severe winter period with snow is now behind us which will improve safety conditions on sites. However, this should not lead to any relaxation as our inherent vulnerability actually remains the same. So, let's make sure we all lead by example and always adopt the safety essentials: STOP, THINK & CHECK, stepping in when we observe any risks or improper behaviour.

I would like to insist on the concept of "keeping oneself out of the line of fire". The very severe incident in Poland, where an employee was crushed against a truck by his loading shovel which rolled away as he fitted a towing bond between the two vehicles, could have been avoided if the concept of "keeping oneself out of the line of fire" had been applied. Towing a vehicle is an exceptional task that should trigger a "Stop, Think & Check" mental reaction rather than trying and doing the task on the fly. No urgency, no economic imperative should lead anyone to put himself/herself at risk.

Let's always think about our own vulnerability and plan properly any non-routine task.
I wish you all a safe week.

Take care.
Michel

Excellent Safety First And Consideration To Other Road Users Near Moota

We received this very reassuring email from a member of public who lives near our Moota Quarry in Cumbria…

"I live in Torpenhow and this afternoon I saw two of your tippers presumably from Moota Quarry. Both were driving carefully and at a reasonable speed. I met one of them when I was walking two dogs that were off the lead. When one of my dogs ran off near the trucks, the driver stopped and waited until I signalled to him that it was safe to proceed. I was impressed. Thank you!"

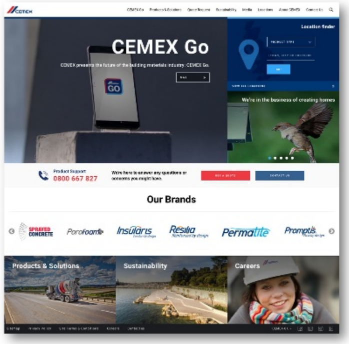
London Readymix Team Holds An Area VFL Day Held In Croydon

Adam Leverett reported that London Readymix held an Area VFL Day on Wednesday 21st March which included Area Managers from other parts of the business. Adam attended a cold but sunny Croydon Plant and was very impressed with Plant Manager, Sam's, induction – it was carried out in the yard and was engaging and informative.

Adam commented: "My IN-CAB VFL with IHC, Kev (over 30 years service) was to a new site for Stilebridge Groundworks in Addiscombe - great service and product and most importantly a very happy customer. Well done to Sam and Chris at the Plant, and Kev - thanks for keeping me safe."

BEING THE BEST FOR CUSTOMERS

Working Lean And Agile On Our New Website – 9 Months Work In 9 Weeks!



CEMEX Go

CEMEX presents the future of the building materials industry: CEMEX Go.

Location finder

We're in the business of creating homes

Product Support 0800 667 827

We're here to answer any questions or concerns you might have.

Our Brands

Products & Solutions

Sustainability

Careers

James Fairclough and James Barnett report that progress is going well on the brand new CEMEX UK website, which is due for launch at the end of March. James Fairclough commented: "The new website look and feel, and platform were prerequisites for our CEMEX Go launch in April. By our first deployment on 30th March we will have completed a nine month project in just nine weeks!

We will be working on fixes for the first month in the live environment and our second deployment will be on 23rd April. We will then move on to a Phase 2 where we will be optimising the content through testing and improvement. This project has only been possible with the use of Agile philosophy- for those interested a modified scrum approach. We have had to be extremely creative with our solutions to make the deadline for the deployment next week... so please bear with us whilst we are working through fixes. However, we would also appreciate feedback and suggestions for moving forward."

Well done team – particularly as much of this work has been "out of hours" due to collaboration with colleagues in Mexico.

Congratulations To Our Bid Team On More Brilliant Project Wins

A big shout out and well done to the submissions team who have not only been part of the tender teams awarded £844,600 worth of work to the CEMEX UK business, they also submitted a further three competitive quality/price tenders and seven Prequalification/Supplier documents within the last ten days!! Submissions Manager, Jenna Swain, said: "People underestimate what it takes to pull these documents together and coordinate various stakeholders across the business." And Aman Kundi also reported they were successful with the A4061 Bwlch-Y-Clawdd Road resurfacing invitation to tender – the project starts on 3rd April.

Thank you to Colin Michael Jones and Paul Lillico from Paving Solutions for investing their time into this bid. Another win for the Submissions Team! - Neale McMaster, Helen Joanne Hart and Jenna Louise Swain.

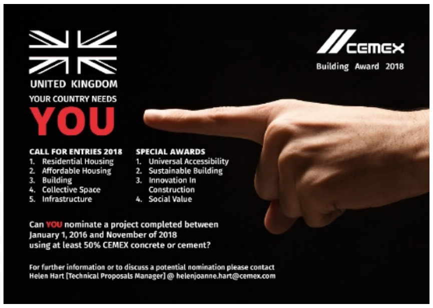
We're Busy Slip-Forming For Stephensons In Cardiff

Not satisfied with the success of Javelin Park Slipforms in the last six months, Stephane Plisson reports that Area 20 is supplying two Slipforms simultaneously for Stephensons in Cardiff City Centre. The thinner section building is planned to become one of the tallest buildings in Cardiff and we are making good progress as you can see in the photo.

Winter has not stopped the construction, in fact, quite the contrary, as we have supplied the vast majority of the project with additional hot water (together with additional associated revenue!).

Thanks to all the team involved, keep going we are nearly there!

Call For Entries – 2018 CEMEX UK Projects For CEMEX Building Award



UNITED KINGDOM

YOUR COUNTRY NEEDS

YOU

CEMEX Building Award 2018

CALL FOR ENTRIES 2018
1. Residential Housing
2. Affordable Housing
3. Building
4. Collective Space
5. Infrastructure

SPECIAL AWARDS
1. Universal Accessibility
2. Sustainable Building
3. Innovation In Construction
4. Social Value

Can YOU nominate a project completed between January 1, 2016 and November of 2018 using at least 50% CEMEX concrete or cement?

For further information or to discuss a potential nomination please contact Helen Hart [Technical Proposals Manager] @ helenjoanne.hart@cemex.com

Helen Hart is asking for any potential entries for the annual CEMEX Building Award in a number of categories as shown on the picture.

The CEMEX Building Award is held each year in Mexico and celebrates excellence in design and use of our materials – projects need to have contained at least 50% CEMEX concrete or cement.

Area 6 RMX Meet Stockton Team – ONE CEMEX

A collaborative workshop with Area 6 RMX and the Accounts Receivable team was held on Wednesday 21st March. The morning session involved a presentation that covered WC, queries (how they impact Aged Debt), payment terms, how they can support AR, how we can support Commercial etc. There was also some training on the Aged Debt tool that is circulated to the business monthly.

The afternoon session involved a review of the overdue debt for the Cluster, including the attendance from five of the Credit Controllers who manage the accounts that have Cluster 6 debt. The Credit Controllers and Sales Executives discussed accounts and surrounding issues from both sides.

The feedback from both teams was very positive. They thought it was engaging and interesting to hear things about the accounts they look after from a different point of view.

2 Weeks To Go!

Find out what is happening in the world of Go in this week's Newsletter. 2 weeks until April's go-live. We have produced a poster for you to put up in the workplace to explain what CEMEX Go is.

Please find it in the download section of the UK News website or at the end of this document.

BEING THE BEST FOR SHAREHOLDERS

Change Of Registered Address – Effective From 4th June 2018

With the impending closure of the Thorpe office and establishment of the Head Office in Rugby, it has been agreed that from **4 June 2018** our new registered office will be:

CEMEX House, Evreux Way, Rugby, Warwickshire CV21 2DT

All necessary changes are in the process of being made by our Legal team, and external parties will be informed. The following changes are also being made:

- **Headed Notepaper -** CEMEX UK headed notepaper used after 4th June 2018 will need to state the correct new registered office address, and old stocks destroyed after that date. New stocks can be obtained in the usual way from our supplier, Banner, who are being made aware of the change.

- **Sales Documents Sent to Customers -** All sales documentation will be updated to include the new registered office address.

- **Email Footer -** An automatic message will be added by Process and IT to all outgoing external CEMEX UK emails, explaining the change to our registered office, and detailing the names and numbers of our principal companies.

- **Terms & Conditions** – Our Terms and Conditions are now kept for reference on our website – these will also be changed for each company to update the new registered address.

BEING THE BEST FOR COMMUNITIES

Simple Idea At Stanwell Improves Security And Engages The Residents

At our Stanwell site we have had a history of trespass and unauthorised use of the access to the old Lodge House which resulted in damage to the listed gates and lots of complaints from the local residents.

Alison came up with an idea of placing old concrete ring segments filled with soils from the recycling operation across the entrance which we filled with flowers last year to help with the Stanwell in bloom celebration. The local residents have since planted daffodils which are now just coming into flower. This has provided great PR and very little cost.

Positive Response To Public Exhibition On Parkfield Road Restoration, Rugby

Plans to transform our disused Parkfield Road Quarry into grassland, ponds and woodland were presented recently when residents were invited to attend a public display of the plans for the site which is close to the Rugby Cement Plant. Ian Southcott, representing CEMEX, said: “These are exciting and imaginative proposals that, if accepted, will transform a deep void into a sustainable and attractive landform with public access.”

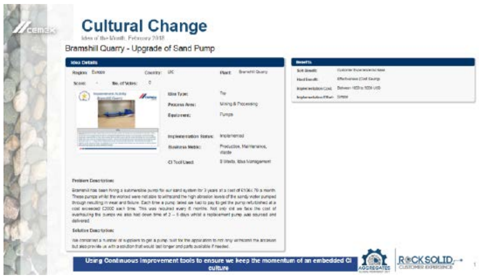
The restoration scheme, which will be the subject of a consultation process undertaken by Warwickshire County Council, would restore the Quarry to its original levels and see the creation of ponds, grassland, open areas for natural re-colonisation and extensive areas of woodland planting.

The site was once a source of raw materials for the cement manufacturing process but has been disused for many decades. One of the public footpaths around the perimeter has been closed for some time and the Quarry is securely fenced for safety reasons. To provide this sustainable, long-term restoration solution, CEMEX is considering bringing in by rail inert materials – clays and soils – from HS2 engineering works. If accepted, these proposals would see this material delivered in trains direct to the existing sidings adjacent to the old Quarry.

The public exhibition took place at the St Matthew’s and St Oswald’s church hall on Lawford Road on Tuesday 20th March. More information at http://www.cemex.co.uk/parkfield-road-quarry-restoration.aspx

BEING THE BEST FOR EMPLOYEES

Bramshill Team Wins Another Global CEMEX Best Idea



Cultural Change

Idea of the Month, February 2018

Bramshill Quarry - Upgrade of Sand Pump

Idea Details

Region: Europe | Country: UK | Plant: Bramshill Quarry

Score: - | No. of Votes: 0

Idea Type: Tip

Process Area: Mining & Processing

Equipment: Pumps

Implementation Status: Implemented

Business Metric: Production, Maintenance, Waste

CI Tool Used: 8 Wastes, Idea Management

Problem Description:

Bramshill has been hiring a submersible pump for our sand system for 3 years at a cost of £1364.79 a month. These pumps whilst the worked were not able to withstand the high abrasion levels of the sandy water pumped through resulting in wear and failure. Each time a pump failed we had to pay to get the pump refurbished at a cost exceeded £2000 each time. This was required every 6 months. Not only did we face the cost of overhauling the pumps we also had down time of 2 – 5 days whilst a replacement pump was sourced and delivered.

Solution Description:

We contacted a number of suppliers to get a pump built for the application to not only withstand the abrasion but also provide us with a solution that would last longer and parts available if needed.

Benefits

Soft Benefit: Customer Experience/Less Waste

Hard Benefit: Effectiveness (Cost Saving)

Implementation Cost: Between 1000 to 5000 USD

Implementation Effort: [illegible]

Using Continuous Improvement tools to ensure we keep the momentum of an embedded CI culture

Congratulations to Bramshill Quarry, who not only won the UK Best Idea for the month but also now the Global Aggregates Best Idea for the month.

They had previously been hiring a submersible pump to work in their sand systems, and recognising the high ongoing cost, found a cheaper and more effective permanent solution.

Craig Hooper commented: “I think this is now three Global Best Ideas in a row for the UK – well done to everyone.”

Security Update….

ACT | ACTION COUNTERS TERRORISM

In these times of heightened threat, and with warmer weather and lighter evenings approaching, MPA has been asked to highlight the latest campaign launched by the National Counter Terrorism Policing under the UK Protect ACT (Action Counters Terrorism) banner. The campaign is designed to encourage the public to report any suspicions about potential attack planning and is seeking the support of the business community across the Great Britain to help defeat terrorism and save lives by reporting suspicious activity and behaviour to police via: www.gov.uk/ACT

The geographic spread of member company interests across the country, means that the mineral products sector are well placed to support this initiative. Consequently, the toolkit in the download section of UK News or at the end of this document, produced by National Counter Terrorism Policing, can be used to raise awareness within your own businesses. Also in the download section of UK News or at the end of this document the guidance produced by the Centre for the Protection of National Infrastructure (a Government agency that reports to the Head of MI5) can be found which provides advice on how to identify and disrupt hostile reconnaissance, and we can further recommend the ‘*Passport to Good Security for Senior Executives*’ produced by the same organisation - https://www.cpni.gov.uk/managing-my-asset/leadership-in-security/board-security-passport

It is important to note that the principles around raising staff awareness to security threats are equally relevant to countering ongoing risks to the supply chain or indeed criminal behaviour in and around members sites and operations more generally.

The threat to the supply chain has certainly not gone away. There is already evidence that tactics employed at the Preston New Road fracking site are now being exported to other parts of the country, and the recent Examination in Public for North Yorkshire’s mineral plan (which included unconventional hydrocarbon extraction) included a significant police presence. There are also recent examples of direct action being undertaken in Europe, with senior executives of an energy company being directly targeted by protestors: http://www.dw.com/en/attack-on-innogy-cfo-not-the-first-in-germany/a-42833597

MPA continue to hold regular meetings with the national police unit responsible for coordinating intelligence on supply chain issues. While any concerns or issues should always be reported directly to the local police in the first instance, the national team has once again encouraged individual member companies to feed any reports of suspicious activity or emerging threats through MPA, via Mark Russell (mark.russell@mineralproducts.org), to support the coordination of the mineral sectors engagement with national police. By channelling information through MPA, this will also ensure that all member companies can be appropriately sighted on any new threats or risks that may be emerging in other parts of the country.

15 Years For Dale Christian

Dale recently completed his 15 years service. Dale's career began in 2003 where he started with our Rail Solutions business in Somercotes. He has spent all his career at Somercotes and enjoys the challenges Rail brings.

Terence Clair, Ops Manager, commented: "It has been an honour to work along Dale and to see him grow over the last 15 years. I am thankful to have Dale with us at Somercotes and it is always reassuring to know that we have people like Dale who are committed to working with us for such a long time."

Thank You And Happy Retirement….

Graham Scott retired on Friday 23rd March after 19½ years in service. He celebrated, with colleagues, with a meal and farewell drink.

We wish Graham farewell and happy retirement.

Congratulations Trevor Moore

Congratulations and thank you Trevor, from Lincs Earthworks team, for reaching 15 years service.

To mark his achievement Trevor was awarded £200 worth of Asda vouchers.

Phil Moore's New Family Addition

Phil Moore, Operations Manager in Area 14, and his partner Sarah, are pleased to announce the safe arrival of their daughter.

Rosie Louise Moore was born on Wednesday 21st March and weighed in at 5lb 8oz, and both Mother and baby are doing fine.

Phil is enjoying some quality time with his addition to the family and both Matthew Yaxley, and the Area team wish Phil, Sarah, and Rosie a long healthy life together along with the sleepless nights.

Internal Vacancies

IVC Ref	Position	Company	Location	Closing date
107-03-2018	Quarry Operative	Aggregates Scotland	Temple Quarry	30/03/2018
108-03-2018	Multi Skilled Operative	Asphalt	Stourton Depot and Coating Plant	10/04/2018
109-03-2018	Weighbridge Operative	Aggregates Central	Cromwell Quarry	11/04/2018
110-03-2018	Assistant Quarry Manager	Aggregates Central	Cromwell Quarry	09/04/2018

For further details on other roles and a full listing of other vacancies, together with information on how to apply, please log on to CEMEX Shift > My Services > Internal Vacancies>New IVCs.

We would love to hear from you for the next edition
To send us a story: either click on 'submit a story' on the UK News website or email
gb-communicationsandpublicaffairs@cemex.com
or call us on 01932 583 217/006

If you can, please include a photo too (taken in super fine landscape setting and saved as a jpeg.) Thank you.

TWO WEEKS TO GO

Your weekly CEMEX Go pre-launch update – 27 March

CEMEX Go Launch Briefings in April – 12th Rugby, 17th Uddingston, 18th Stockton, 23rd Preston Brook

Another reminder that we'll be holding CEMEX Go launch briefings at the above sites during April with everyone welcome to attend. We're planning at least two sessions am and pm at each event and will run more if required. The objective is to spread the word about CEMEX Go, ensuring everyone knows what is happening, when it will happen in their business, how they can support the initiative, and most importantly the benefits to our customers. The Rugby sessions on 12th April will be in 8th Floor meeting room at 10am, 12 noon, 2pm and 4pm.

Successful CEMEX Go Readymix IHC Engagement Session in Bristol

Rob Sims and Adam Leverett delivered another very successful engagement session on Wednesday evening with our local independent haulage contractors (IHC) drivers in the Bristol area. Our readymix business is going live in regional phases, with the North West and South West areas first. Our digital support team have also attended both events to collect the valuable feedback from the drivers to share with the wider business and help answer questions

Three readymix customers confirmed for CEMEX Go launch in North West

We were delighted this week to sign up **three readymix customers** for the north-west CEMEX Go launch release – left to right – 1. Andrew Livesey of **John Turner Construction** - the main service that interested Andrew was Track. 2. **Raised Floor Solutions** who want to use the full end-to-end CEMEX Go service, and are excited for the launch. 3. **Technic Concrete Floors** – managing director Darren said they have Track on their own vehicles and is excited both about CEMEX Go and the future of CEMEX!.

Action Counters Terrorism 2018 Campaign Toolkit

Communities Defeat Terrorism: reporting suspicious activity & behaviour

Overview

Thank you for supporting the 2018 ACT (Action Counters Terrorism) public awareness campaign, which will launch on Tuesday 20 March and run for four weeks.

Communities defeat terrorism and with the enduring terrorist threat, it is now more important than ever that everyone plays their part in tackling terrorism. Individual actions could save lives.

That's why the ACT campaign is encouraging the public to help the police tackle terrorism and save lives by reporting suspicious behaviour and activity at www.gov.uk/ACT. We will be raising awareness of the different attack planning methods that terrorists might use so the public knows some of the signs to spot and how to report any concerns.

This campaign toolkit will provide you with the background and resources you need to support the campaign.

You can download all of the campaign resources via WeTransfer.

Please note that all of this material is under embargo and should not be used publicly until 00:01 Tuesday 20 March 2018.

How you can help:

- Adapt our news story template for your website about why you're supporting ACT and share examples of signs to spot and how to report **(p5)**
- Share ACT posters and graphics in your organisation's building, display screens and public areas **(p11)**
- Share our digital assets and creative film on your organisation's social media accounts **(p5)**
- Provide a supportive statement from your organisation for the ACT campaign **(p2)**
- Use external newsletters, your website, blogs and other channels to signpost the public to advice on how to report suspicious activity or behaviour that could be terrorist related via www.gov.uk/ACT **(p5 & p11)**
- Use staff newsletters and your intranet to signpost internal staff to advice on how to report suspicious activity or behaviour that could be terrorist related via www.gov.uk/ACT **(p9)**

If you have any comments or questions, or require access to the content in a different format please contact us on nctphq.comms@met.police.uk

Table of Contents

About Counter Terrorism Policing

Counter Terrorism Policing is a collaboration of UK police forces working alongside the UK intelligence agencies to protect the public and our national infrastructure. Our officers and staff are at the frontline of the UK's fight against terrorism, working tirelessly to prevent, disrupt and investigate extremists, whatever their ideology.

ACT Background

In March 2017, National Counter Terrorism Policing launched ACT (Action Counters Terrorism), a new branding platform which incorporates all of our counter-terrorism external campaigns to warn, inform and reassure the public.

Make Nothing Happen was the first national advertising campaign to be launched under ACT. Its objective of encouraging the public to trust their instincts to report anything they see or hear which may be terrorist related, was underpinned by the message that cooperation between the public and the police remains the greatest advantage in tackling the challenges the UK faces from terrorism. The campaign ran across radio and digital channels over six weeks (of paid for activity) backed by a national and regional media and PR plan.

Since the launch of *Make Nothing Happen* in March 2017, there have been five terrorist attacks in the UK resulting in a change of rhythm and tempo in police investigations. As a result, there is now less need to remind people of the terrorist threat. Instead we must continue to find ways of educating the public about the different methods of attack planning beyond 'the suspicious package' while encouraging them to be part of the Counter Terrorism effort to help us stop attacks happening in the first place.

2018 ACT Campaign Objectives

The campaign's objectives are:

- Encourage the public to report suspicious activity or behaviour and increase intelligence from communities.

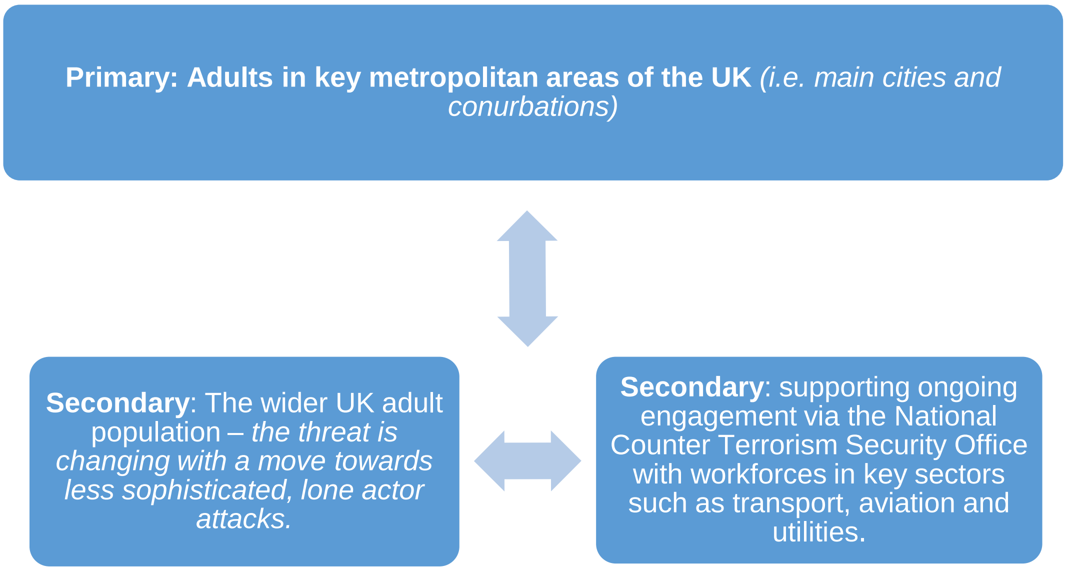
- Increase public understanding of what activity or behaviour to look out for by highlighting examples of terrorist attack planning methods.

- Increase awareness of key reporting channels like gov.uk/ACT.

- Reinforce the message that communities defeat terrorism – and the key role the public have to play in helping tackle the terrorist threat.

Target Audiences

The main audiences the campaign will target are:



Primary: Adults in key metropolitan areas of the UK *(i.e. main cities and conurbations)*

Secondary: The wider UK adult population – *the threat is changing with a move towards less sophisticated, lone actor attacks.*

Secondary: supporting ongoing engagement via the National Counter Terrorism Security Office with workforces in key sectors such as transport, aviation and utilities.

Audience Insight

In January 2018, an online study, with over 1,000 UK adults across the country.
The pre-campaign research found:

- Anxiety over terrorism in the UK is high (**83%**) with a third of the public saying they are very concerned. **Two-thirds** say they have become more concerned over the past year, which has been fuelled by the frequency and unpredictability of attacks.
- **3 in 4** feel the police are doing well in keeping the public safe, believing that much work goes on behind the scenes to thwart potential attacks.
- The **vast majority** would report suspicious behaviours with being 'safe rather than sorry' as a key motivator.
- The motivation to report suspicious behaviour is high at **82%**, with the potential to save lives being a strong driver.
- A **very small number** of people would not report and their main barriers included fear of getting someone into trouble if incorrect, distrust of the police and fear of wasting police time.
- Extreme behaviours such as an interest/use of in firearms or chemicals are **easier** for people to label as a high threat, but they are **less certain** about the behaviours that are more everyday/potentially ambiguous.
- **Online search** is the first port of call to find out more information or advice on reporting suspicious activity.
- More than **1 in 10** are aware of ACT which is good considering that it is a very new brand. However awareness is lower than other reporting methods, so raising awareness will be a key function of this campaign.
- The reporting methods that are **seen as easy to use** are favoured, but this preference is subjective (i.e. preferring to speak over the phone) and subject to interpretation (i.e. some people saw reporting suspicious behaviour as an emergency (and there requiring a 999 response) whereas others did not).

Key Messages

- Communities defeat terrorism.

- Like other criminals, terrorists need to plan. If you see or hear something unusual or suspicious trust your instincts and ACT by reporting it in confidence at gov.uk/ACT.

- Any piece of information could be important, it is better to be safe and report. You can help the police prevent terrorism and save lives.

- You are not wasting our time, and we will only take action after the appropriate checks have been carried out.

2018 ACT Campaign Narrative

Communities defeat terrorism. With the enduring terrorist threat, it is now more important than ever that everyone plays their part in tackling terrorism. Your actions could save lives.

That's why Action Counters Terrorism (ACT) is encouraging communities across the country to help the police tackle terrorism and save lives by reporting suspicious behaviour and activity.

Like other criminals, terrorists need to plan. If you see or hear something unusual or suspicious trust your instincts and ACT by reporting it in confidence at gov.uk/ACT or, in an emergency, dial 999.

Some examples of suspicious activity or behaviour could potentially include:

- Hiring large vehicles or similar for no obvious reasons
- Buying or storing a large amount of chemicals, fertilisers or gas cylinders for no obvious reasons
- Taking notes or photos of security arrangements, or inspecting CCTV cameras in an unusual way
- Looking at extremist material, including on the so-called Dark Web, or sharing and creating content that promotes or glorifies terrorism.
- Someone receiving deliveries for unusual items bought online.
- Embracing or actively promoting hateful ideas or an extremist ideology.
- Possessing firearms or other weapons or showing an interest in obtaining them
- Holding passports or other documents in different names, for no obvious reasons
- Anyone who goes away travelling for long periods of time but is vague about where
- Someone carrying out suspicious or unusual bank transactions

You are not wasting our time, and no call or click will be ignored. What you tell us is treated in the strictest confidence and is thoroughly researched by experienced officers before, and if, any police action is taken.

Any piece of information could be important, it is better to be safe and report. Remember, trust your instincts and ACT. **Action Counters Terrorism**.

Campaign Strategy

Counter Terrorism Policing will launch the 2018 ACT campaign on 20 March 2018. This campaign will run over a four week period and will deliver an integrated communication approach to maximise message reach including:

- **Paid for digital advertising:** a paid for online video campaign to maximise exposure and reach (targeted at specific areas informed by operational policing) will run for four weeks. This will include a new creative film to educate the public on different attack planning methods to look out for and explain how reporting suspicious behaviour and activity can help the police tackle terrorism and keep communities safe.

- **Owned and earned channels:** share engaging content with clear call to action via: the Counter Terrorism network and police forces' channels and stakeholder networks; Government and GCS local channels and stakeholder networks; and mainstream, regional, specialist and online media.

- **Media:** A full media plan and resources can be found on page 10 and includes national, regional and local activity supplemented by editorial engagement with national, BME, consumer and regional press and broadcasters.

- **Digital and social media:** campaign activity across owned, borrowed and paid for channels, police force/Government/local authority and other key stakeholder websites, social media accounts and video broadcasting channels.

We will be seeking your help in sharing the messaging across your own channels and networks to help us maximise our reach.

Evaluation

To evaluate the impact of the campaign, we will be measuring a range of factors to understand which tactics and channels most effectively raised awareness of the ACT campaign and encouraged the public to report suspicious behaviour and activity.

Our primary measurement will be the number of calls and online reports we receive from the police and the proportion of those that become actionable intelligence.

However, we ask that once the campaign concludes, if partners could share the following information to help us evaluate the campaign:

- Social media engagement on your native posts about ACT (i.e. Facebook, Twitter, Instagram, etc)
- If you signposted ACT on your external website
- If you signposted ACT on your intranet
- If you signposted ACT in your newsletters/external communications
- If you signposted ACT via posters or display screens in your building
- Any media coverage you secured on ACT

We would be grateful if you could share any of the above examples with the campaigns team on nctphq.comms@met.pnn.police.uk.

Digital Resources

We will be using all of our social media channels to promote the creative film, share informational graphics and direct the public to www.gov.uk/ACT which provides a one stop shop for the online reporting tool, advice, campaign materials and links to supportive information.

How can you support online?

- We have provided **graphics, still images, a film and suggested social media posts** that you can share across your social media channels.
- We have provided a **template news story** that you can publish on your website, educating the public on where to report and what to look out for.
- We have provided **suggested website wording** for your organisation's pages on counter terrorism for you to review and update.

The campaign's hashtag is #ActionCountersTerrorism

Our social media channels are:

- Twitter: @TerrorismPolice
- Facebook: @CounterTerrorismPoliceUK
- Youtube: https://www.youtube.com/counterterrorismpolicinguk

We encourage you to support not only on the channels above, but on any other channels your organisation might have, such as Instagram, Snapchat and other social media networks.

*Please note that the Anti-Terrorist Hotline textphone option for the deaf or hard of hearing is no longer in service. **Please remove this if it is still on your website**.*

ACT Campaign Film

You can view, share and embed the ACT film from YouTube and download it here under the file name *ACT-Film* or alternatively the file name *ACT-Film-Social* which is formatted in a 16:9 ratio for your social media channels:

We encourage all of our partners to share it across your social media channels using the hashtag #ActionCountersTerrorism. We have included a suggested post below, but please tailor it to your audiences.

Twitter

Tweet One

It's more important than ever that everyone plays their part in tackling terrorism. Any piece of information could be important. You can help prevent terrorism and save lives. Trust your instincts and ACT. Visit www.gov.uk/ACT #ActionCountersTerrorism

[Insert video **ACT-Film-Social.mp4** or link to **https://youtu.be/l6SjX2ZXMnY**]

Tweet Two

We support @terrorismpolice encouraging everyone to play their part in tackling terrorism. Any piece of information could be important and help save lives. Trust your instincts and ACT. Visit www.gov.uk/ACT #ActionCountersTerrorism

[Insert video **ACT-Film-Social.mp4** or link to **https://youtu.be/l6SjX2ZXMnY**]

Facebook

Communities Defeat Terrorism

It’s more important than ever that everyone plays their part in tackling terrorism. Your actions could help police prevent terrorism and save lives.

Like other criminals, terrorists need to plan. If you see or hear something unusual or suspicious trust your instincts and ACT by reporting it in confidence at gov.uk/ACT.

Any piece of information could be important, it is better to be safe and report. #**ActionCountersTerrorism**.

[Insert video **ACT-Film-Social.mp4** or link to **https://youtu.be/I6SjX2ZXMnY**]

Social media content

You can download all of the social media graphics

To note that this link will only be live for a week. If you need to download the graphics after that point, please email the communications team on nctphq.comms@met.pnn.police.uk**.**

Included below are suggested posts for each of the graphics. We encourage you to share these on your channels natively and tailoring it to your audiences.

Suggested post	Content File Name
If you see or hear something suspicious trust your instincts and ACT by reporting it in confidence at www.gov.uk/ACT #ActionCountersTerrorism	*Social-Twitter-1.png / social-campaign-image-1.png*
It only takes a moment to report suspicious activity online. You could help prevent an attack and save lives. Trust your instincts and ACT by reporting it at www.gov.uk/ACT #ActionCountersTerrorism	*Social-Twitter-2.png / social-campaign-image2.png*
Your actions could save lives. Reports from the public have foiled terrorist plots. Trust your instincts and ACT by reporting it in confidence at www.gov.uk/ACT #ActionCountersTerrorism	*Social-Twitter-3.png / social-campaign-image3.png*
Any piece of information could be important, it is better to be safe and report. You can help the police prevent terrorism and save lives. Visit www.gov.uk/ACT #ActionCountersTerorrism	*Social-Twitter-4.png / social-campaign-image4.png*

You can help tackle terrorism. If you spot anything suspicious online, report it. Visit www.gov.uk/ACT #ActionCountersTerrorism	*Social-Suspicious-Online-Animation.gif* *Social-Suspicious-Online-Video.mp4*
Terrorists need to plan. If you see or hear about someone who has, or is trying to, access illegal firearms and weapons report it. Visit www.gov.uk/ACT #ActionCountersTerrorism	*Social-Suspicious-Weapons-Animation.gif* *Social-Suspicious-Weapons-Video.mp4*

Trackable website links

To help our campaign evaluation, we've created bespoke trackable google links to Gov.uk for each of our partner groups to measure where most of the gov.uk/ACT traffic comes from. Please use the links below on your websites or in your online content.

- Local Authorities: https://www.gov.uk/ACT?utm_source=la
- UK Government Departments & ALBs: https://www.gov.uk/ACT?utm_source=gov
- UK Law Enforcement (Police Forces, NCA, etc): https://www.gov.uk/ACT?utm_source=ukpol

Please ensure that when using these links, they are visible only as **gov.uk/ACT**

Suggested website wording on counter terrorism

If your website has a dedicated page to counter terrorism, then we have provided some suggested content in a guide that you can tailor to your local audiences. You can download the guide under the file name *Website-CT-Content* here.

Template Website News Article

Action Counters Terrorism: Report suspicious activity and behaviour to tackle terrorism

[INSERT ORGANISATION] urges the public to help the police tackle terrorism and save lives by reporting suspicious behaviour and activity.

Communities defeat terrorism. With the enduring terrorist threat, it is now more important than ever that everyone plays their part in tackling terrorism. Your actions could save lives.

Don't worry about wasting police time. No call or click will be ignored. What you tell the police is treated in the strictest confidence and is thoroughly researched by experienced officers before, and if, any police action is taken.

Any piece of information could be important, it is better to be safe and report. Remember, trust your instincts and ACT. **Action Counters Terrorism.**

How can I report?

Reporting is quick and easy. You can report in confidence **online** via our secure form: www.gov.uk/ACT. Alternatively, you can call the police confidentially on 0800 789 321.

All reports are kept confidential and you can report anonymously.

In an emergency always call 999.

What should I report?

Like other criminals, terrorists need to plan. You can report suspicious activity or behaviour – anything that seems out of place, unusual or just doesn't seem to fit in with everyday life.

Watch the ACT film to learn more:

[*EMBED FILM* - https://youtu.be/I6SjX2ZXMnY]

What could potentially be terrorist-relates suspicious activity or behaviour?

Research

Meetings, training and planning can take place anywhere. Do you know someone who travels but is vague about where they're going?

Do you know someone with passports or other documents in different names, for no obvious reason?

Do you know someone who looks at extremist material, including on the so-called Dark Web, or shares and creates content that promotes or glorifies terrorism?

Have you noticed someone embracing or actively promoting hateful ideas or an extremist ideology?

Gathering materials

Suspicious materials can be ordered online as well as in store. Have you noticed someone receiving deliveries for unusual items bought online?

If you work in commercial vehicle hire or sales, has a sale or rental seemed unusual?

Have you noticed someone buying large or unusual quantities of chemicals, fertilisers or gas cylinders for no obvious reason?

Have you noticed someone acquiring illegal firearms or other weapons or showing an interest in obtaining them?

Storing materials

Terrorists need to store equipment while preparing for an attack. Have you noticed anyone storing large amounts of chemicals, fertilisers or gas cylinders?

Have you noticed anyone storing illegal firearms or objects that could potentially be weapons?

Hostile Reconnaissance

Observation and surveillance help terrorists plan attacks. Have you witnessed anyone taking pictures or notes of security arrangements or CCTV?

Financing

Cheque and credit card fraud are ways of generating cash. Have you noticed any suspicious or unusual bank transactions?

If you'd like more information or resources, visit www.gov.uk/ACT or follow Counter Terrorism Policing on social media:

- Facebook
- Twitter
- YouTube
- #ActionCountersTerrorism

Internal communications resources

In addition to promoting the campaign to external audiences, we are also providing resources to signpost your staff to advice on how to report suspicious behaviour and activity that could be terrorist related.

How can you support?

- We've provided a template article text for you to adapt for your intranet or internal staff newsletters.
- We have also provided graphics for you to display on your building's display screens.
- Share the ACT film on your intranet for your staff to see

ACT Campaign Film

You can view and share the ACT film from YouTube and download it here. If you require the video in a different format, please email nctphq.comms@met.pnn.police.uk

Display screen graphics

You can download the following graphics to use on your building's display screens and website:

These images can be used on your display screens:

- 1080x1920 Image → *Digital-Display-Screen-Image-Vertical*
- 16:9 MP4 → *Digital-Display-Screen-Movie-169*

We have also provided a series of GIFs for Local Authorities to use on their advertising filler service under the following names:

- 160x600 GIF → *Local-Authority-Website-Advert-1*
- 300x250 GIF → *Local-Authority-Website-Advert-2*
- 320x50 GIF → *Local-Authority-Website-Advert-3*
- 728x90 GIF → *Local-Authority-Website-Advert-4*

Template Intranet/Newsletter text – 2018 ACT Campaign

[*Insert organisation*] is proud to support Counter Terrorism Policing's Action Counters Terrorism (ACT Campaign) to encourage the public to help the police tackle terrorism and save lives by reporting suspicious behaviour and activity.

Communities defeat terrorism. With the enduring terrorist threat, it is now more important than ever that everyone – including [*insert organisation*] staff – plays their part in tackling terrorism. Our actions could save lives.

Like other criminals, terrorists need to plan. If you see or hear something unusual or suspicious trust your instincts and ACT by reporting it in confidence at gov.uk/ACT. If it's an emergency call 999.

Watch the ACT film to learn more:

[*EMBED FILM* - https://youtu.be/I6SjX2ZXMnY]

What could potentially be terrorist-related suspicious activity or behaviour?

Research

Meetings, training and planning can take place anywhere. Do you know someone who travels but is vague about where they're going?

Do you know someone with passports or other documents in different names, for no obvious reason?

Do you know someone who looks at extremist material, including on the so-called Dark Web, or shares and creates content that promotes or glorifies terrorism?

Have you noticed someone embracing or actively promoting hateful ideas or an extremist ideology?

Gathering materials

Suspicious materials can be ordered online as well as in store. Have you noticed someone receiving deliveries for unusual items bought online?

If you work in commercial vehicle hire or sales, has a sale or rental seemed unusual?

Have you noticed someone buying large or unusual quantities of chemicals, fertilisers or gas cylinders for no obvious reason?

Have you noticed someone acquiring illegal firearms or other weapons or showing an interest in obtaining them?

Storing materials

Terrorists need to store equipment while preparing for an attack. Have you noticed anyone storing large amounts of chemicals, fertilisers or gas cylinders?

Have you noticed anyone storing illegal firearms or objects that could potentially be weapons?

Hostile Reconnaissance

Observation and surveillance help terrorists plan attacks. Have you witnessed anyone taking pictures or notes of security arrangements or CCTV?

Financing

Cheque and credit card fraud are ways of generating cash. Have you noticed any suspicious or unusual bank transactions?

Don't worry about wasting police time. Any piece of information could be important and it is better to be safe and report. No call or click will be ignored. What you tell the police is treated in the strictest confidence and is thoroughly researched by experienced officers before, and if, any police action is taken.

Remember, trust your instincts and ACT. **Action Counters Terrorism**.

Print Resources

You can also use the following posters and leaflets to display inside your organisation's building. They have been provided in PDF and InDesign formats should you need to resize the image or add your organisation's logo.

The resources can be downloaded here and the relevant file names are below:

A3 Campaign Poster

- *Print-A3*
- *Print-A3-Design*
- *Print-A3-Welsh*

A4 Campaign Poster

- *Print-A4*
- *Print-A4-Design*
- *Print-A4-Welsh*

A5 Leaflet

- *Print-A5*
- *Print-A5-Design*
- *Print-A5-Welsh*

A6 Leaflet

- *Print-A6*
- *Print-A6-Design*
- *Print-A6-Welsh*

ACT logos

The logos below can be used for promoting the campaign. They can be downloaded here.

- ACT Logo Blue: *Logo-ACT-1*
- ACT Logo White: *Logo-ACT-2*
- CT Policing Logo Blue: *Logo-CTP-1*
- CT Policing Logo White: *Logo-CTP-2*

Branding Guidelines

We have also provided guidelines with helpful information on how to use the ACT logo and branding. You can download the *ACT-Brand-Identity-Guidelines-1* here.

Press and Media Resources

The campaign activity will be spread across four weeks, each with a distinct 'theme', outlined below:

- **Week One (20th to 25th March):** Initial campaign launch ahead
- **Week Two (26th March to 1st April):** Communities defeat terrorism
- **Week Three (2nd to 8th April):** Online extremism
- **Week Four (9th to 18th April):** Business and industry

Outlined below are some of the planned activity for each of the four weeks of the campaign. To note that these plans are subject to change.

Pre-launch activity (5th-18th March): Press release (with option to regionalise), delivery plan and social media toolkit delivered to regional comms teams, force press offices and key stakeholders. All under embargo for **00:001hrs Tuesday, 20th March**.

Week One (20th to 25th March): Initial campaign launch ahead of Westminster attack 1st anniversary – content aimed at UK adult population, key stakeholders and partners.

Week Two (26th March to 1st April): Communities defeat terrorism – messaging tailored to bespoke audience including women, LGBT & BAME community and faith groups.

Week Three (2nd to 8th April): Online extremism - targeting UK adult population and sector-specific media to highlight the significance of reporting extremist content online.

Week Four (9th to 18th April): Business and Industry – focusing on the commercial sector and trade publications to demonstrate the collaboration between police and industry as they work to protect communities and infrastructure from terrorism.

Press Notice

Included below is the national press release that has been shared under embargo until 00:01 Tuesday 20 March 2018. This can be tailored by regional police forces for local media.

The new head of UK Counter Terrorism Policing has used the launch of a campaign about terrorist attack planning methods to reveal that more than a fifth of reports from the public produce intelligence which is helpful to police.

The recently appointed Assistant Commissioner of Specialist Operations (ACSO), Neil Basu, praised the public's willingness to ***ACT*** in response to last year's unprecedented rise in terrorist activity, which resulted in record numbers of people contacting the police through online referral forms and the confidential hotline to report suspicious behaviour and activity.
Now he is launching the second phase of the '***ACT*** –Action Counters Terrorism' campaign, featuring a new 60-second film based on real life foiled plots, which will show examples of terrorist-related suspicious activity and behavior, as well as attack planning methodology.

A call to action will encourage the public to report suspicious behaviour and activity via the online tool (gov.uk/ACT), helping the police to prevent terrorism and save lives.

"We have been saying for some time now that communities defeat terrorism, and these figures demonstrate just how important members of the public are in the fight to keep our country safe," says ACSO Neil Basu.

"Since the beginning of 2017 we have foiled 10 Islamist and four right wing terror plots, and there is no doubt in my mind that would have been impossible to do without relevant information from the public."

Of the nearly 31000 public reports to Counter Terrorism (CT) Policing during 2017, more than 6600 (21.2%) resulted in useful intelligence - information which is used by UK officers to inform live investigations or help build an intelligence picture of an individual or group.

Research carried out by CT Policing suggests that while more than 80% of people are motivated to report suspicious activity or behaviour, many are unclear exactly what they should be looking for.

The second phase of the '***ACT*** –Action Counters Terrorism' from CT Policing aims to educate the public about terrorist attack planning and reinforce the message that any piece of information, no matter how small, could make the difference between a lethal attack or a successful disruption.

"Like other criminals, terrorists need to plan and that creates opportunities for police and the security services to discover and stop these attacks before they happen" says ACSO Basu.

"But we need your help to exploit these opportunities, so if you see or hear something unusual or suspicious trust your instincts and ***ACT*** by reporting it in confidence by phone or online.

"That could be someone buying or storing chemicals, fertilisers or gas cylinders for no obvious reasons, or receiving deliveries for unusual items, it could be someone embracing extremist ideology, or searching for such material online.

"This new film has been made to try and help people understand recent terrorist attack-planning methods, but also to demonstrate that each report from the public can be one vital piece of a much larger picture.

"The important thing for people to remember is that no report is a waste of our time, trust your instincts and tell us if something doesn't feel right."

XXXX BEN WALLACE QUOTE XXXX

Notes to Editors:

ACT Background

In March 2017, National Counter Terrorism Policing launched ACT (Action Counters Terrorism), a new branding platform which incorporates all of our counter-terrorism external campaigns to warn, inform and reassure the public.

Make Nothing Happen was the first national advertising campaign to be launched under ACT. Its objective of encouraging the public to trust their instincts to report anything they see or hear which may be terrorist related, was underpinned by the message that cooperation between the public and the police remains the greatest advantage in tackling the challenges the UK faces from terrorism. The campaign ran across radio and digital channels over six weeks (of paid for activity) backed by a national and regional media and PR plan.

2018 ACT Campaign Narrative

Communities defeat terrorism. With the enduring terrorist threat, it is now more important than ever that everyone plays their part in tackling terrorism. Your actions could save lives.

That's why Action Counters Terrorism (ACT) is encouraging communities across the country to help the police tackle terrorism and save lives by reporting suspicious behaviour and activity.

Like other criminals, terrorists need to plan. If you see or hear something unusual or suspicious trust your instincts and ACT by reporting it in confidence at gov.uk/ACT or, in an emergency, dial 999.

Some examples of suspicious activity or behaviour could potentially include:

- Hiring large vehicles or similar for no obvious reasons
- Buying or storing a large amount of chemicals, fertilisers or gas cylinders for no obvious reasons

- Taking notes or photos of security arrangements, or inspecting CCTV cameras in an unusual way
- Looking at extremist material, including on the so-called Dark Web, or sharing and creating content that promotes or glorifies terrorism.
- Someone receiving deliveries for unusual items bought online.
- Embracing or actively promoting hateful ideas or an extremist ideology.
- Possessing firearms or other weapons or showing an interest in obtaining them
- Holding passports or other documents in different names, for no obvious reasons
- Anyone who goes away travelling for long periods of time but is vague about where
- Someone carrying out suspicious or unusual bank transactions

You are not wasting our time, and no call or click will be ignored. What you tell us is treated in the strictest confidence and is thoroughly researched by experienced officers before, and if, any police action is taken.

Any piece of information could be important, it is better to be safe and report. Remember, trust your instincts and ACT. **Action Counters Terrorism**.

2017 Reporting Statistics

- A total of 22955 reports were made to Counter Terrorism Police via the Anti-Terror Hotline. Of which, 5074 resulted in useful intelligence for the police, a conversion rate of 22.1%

- A total of 8029 reports were made to Counter Terrorism Police via online reporting forms at gov.uk/ACT. Of which, 1585 resulted in useful intelligence for the police, a conversion rate of 19.7%

- Cumulatively, 30984 reports were made to Counter Terrorism Police in 2017, of which 6659 (21.5%) resulted in useful intelligence for the police.

Case Studies

North West

- A member of the public reported their concerns online about the content of a publicly accessible Google+ social media account in the name of Abdur-Rahman Salford, which contained lots of material linked to the terrorist organisation Islamic State and material believed to encourage others to commit, prepare or instigate acts of terrorism . The operator of the account, Adam Wyatt, was arrested and has since pleaded guilty.

- Threatening and offensive messages on a Facebook group were seen by a member of the public who alerted the police. As a result of the reporting, far right supporter Ethan Stables was arrested for threatening to kill people attending a local LGBTQ event in Cumbria.

West Midlands

- A member of the public reported a man acting suspiciously near to a school in Birmingham. Upon arrest by officers at the scene, the man was found to be in possession of a large kitchen knife and a crowbar. A search of the man revealed hostile reconnaissance material (hand drawn map), a recipe for explosives and messages on his phone from contacts linked to the proscribed organisation known as ISIL. A search of his address revealed further attack planning materials such as adapted electrical lights, bottles of hydrogen peroxide, wires and dismantled mobile telephones. He was found guilty under section 5 Terrorism Act 2006 on 22nd June 2016 and then sentenced on 9th October 2017 for 15 years in Prison.

FAQs

What type of behaviour or activity could be considered suspicious?

Some examples of suspicious behaviour or activity include:

- Hiring large vehicles or similar for no obvious reasons
- Buying or storing a large amount of chemicals, fertilisers or gas cylinders for no obvious reasons
- Taking notes or photos of security arrangements, or inspecting CCTV cameras in an unusual way
- Looking at extremist material, including on the so-called Dark Web, or sharing and creating content that promotes or glorifies terrorism.
- Someone receiving deliveries for unusual items bought online.
- Embracing or actively promoting hateful ideas or an extremist ideology.
- Possessing firearms or other weapons or showing an interest in obtaining them
- Holding passports or other documents in different names, for no obvious reasons
- Anyone who goes away travelling for long periods of time but is vague about where
- Someone carrying out suspicious or unusual bank transactions

How sure do I have to be before passing on my suspicions?

An honest held belief that something is occurring or you have a belief someone is acting suspiciously.

If my information turns out to be incorrect will I have wasted police time?

You may feel it’s probably nothing, but unless you trust your instincts and tell us we won’t be able to judge whether the information you have is important or not.

Remember, no piece of information is considered too small or insignificant. Our specially trained officers and police staff would rather take lots of calls which are made in good faith, but have innocent explanations, than not getting any at all.

How do I report suspicious behaviour or activity?

You can quickly and anonymously report online via www.gov.uk/ACT or you can call the police in confidence on 0800 789 321. Remember, in an emergency you should always call 999.

Who will take my call or read my online report?

A Counter Terrorism Police Officer or a trained member of police staff will review your information within two hours.

Do I have to give my name or any personal details?

No, it is entirely up to you if you wish to leave your contact details.

Is it confidential?

Yes, all of the information you provide is treated in the strictest confidence. You don’t have to give your details unless you wish to do so.

What if I am concerned that someone will find out I have contacted the police?

We understand that people might have reservations about contacting police, either because their friends or family may find out, or their suspicions may prove to have innocent explanations. But we can reassure you that all calls and information are treated in the strictest confidence and will not be made public.

What sort of detail will the police need from me?

If you are reporting an incident you have witnessed we will need as much detail as possible, this could include the clothing someone was wearing, their age, height, ethnicity and actions for example.

Will my call be traced or recorded?

Your call will not be recorded. If you wish to leave your details you can do so but otherwise your call will remain anonymous.

How long will reporting take?

It will depend on how much information you are able to provide when you contact us.

What will happen with the information?

Our specially trained officers and police staff who take the calls will assess and evaluate the information you pass on before deciding on what action to take.

Will I be given an update?

Unfortunately we are unable to provide updates due to data protection issues and because the information we receive is passed to us on an anonymous basis.

If the police need to speak to me again, how will they contact me?

We will only get in touch with you if we need to ask you further details about the information you have provided. You will have the option to provide your contact details.

Will I need to give a statement?

In a case where you are giving information and wish to leave your contact details, you may be asked to provide a statement however this will depend on your wishes.

Does the hotline have a language line?

If you have difficulties speaking English, you can ask a friend who can speak English to contact us on your behalf. However, we will need to take into consideration the type of call and the privacy and level of information being divulged.

I suffer from hearing loss, how can I pass on information which I think may be important?

Yes, you can also contact the hotline online via www.gov.uk/ACT.

Can I report my suspicions over the phone rather than online?

Yes, if you would prefer to report information over the phone rather than online, you can call the police in confidence you on 0800 789 321.

Will I get a reward if I pass on information to the hotline?

You will not get a reward if you pass on information to the hotline.

If I don’t want to contact police is there anyone else I can talk to?

Family or trusted friends can report on your behalf but we will need to confirm the details provided with you.

You can also report crime or information online or via Crimestoppers anonymously on 0800 555 111
Always remember, if it is an emergency, call 999.

CPNI
Centre for the Protection
of National Infrastructure

HOSTILE RECONNAISSANCE

Understanding and countering the threat

June 2016

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation, or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Contents

Overview and aim of this guidance

Hostile reconnaissance, the term given to the information gathering phase by those individuals or groups with malicious intent, is a vital component of the attack planning process.

Based on over five years of research and extensive testing and evaluation, this guidance gives security managers an understanding of why and how hostile reconnaissance is conducted, and the principles of how to disrupt threats during the reconnaissance phase, along with practical measures on how to reduce the vulnerability of their site.

Critically, the approaches and suite of tools provided in this guidance have been carefully developed to disrupt hostile reconnaissance while having a neutral, informing or even reassuring and recruiting effect on the normal site user. They also focus on utilising existing protective security resources such as CCTV control rooms, security officers and other important resources, such as corporate communications and employees, more effectively to disrupt hostile reconnaissance.

This guidance first provides an overview of hostile reconnaissance in the context of the attack planning process: how to consider the threats an organisation faces from this perspective, the hostile's information requirements, where they will get this information from and how they feel when doing so.

With this understanding, the guidance then provides the Centre for the Protection of National Infrastructure's (CPNI) principles of disrupting hostile reconnaissance: **Deny**, **Detect** and **Deter**. It explains how understanding these, in combination with a recognition of the threat, can help determine an organisation's current vulnerability to hostile reconnaissance and what can be done to counter this.

The final section includes a checklist to provide a method of assessing a site's vulnerability to hostile reconnaissance.

This guidance uses the term 'hostile' to refer to the individual or group conducting the reconnaissance.

Hostile reconnaissance: understanding the threat

Parties conducting hostile reconnaissance; its place in the attack planning process and the opportunity to disrupt.

Organisations face a variety of threats: terrorists, activists, corporate or state-sponsored spies and criminals scrutinise potential targets from near and far.

But while these threats and their aims may vary, hostiles are united in their desire to succeed. Recognising they may not get a second chance to achieve their aims, hostiles will typically plan carefully.

By using online research, on-site visits and, if and where necessary, insider knowledge, the hostile will try to obtain enough detailed information and get sufficient certainty about the reliability of this information to inform their modus operandi and be sure of success.

This activity can be described as hostile reconnaissance. CPNI defines it as "Purposeful observation with the intention of collecting information to inform the planning of a hostile act against a specific target."

Generally, the more sophisticated the attack the more complex the attack planning, and consequently the greater the information requirement and reconnaissance need. The information gathered is typically used by hostiles to assess the state of security and likelihood of detection; to assess vulnerabilities in security and to assess likelihood of success.

Understanding this gives security managers an absolutely crucial opportunity to disrupt by creating a perception and/or assessment of failure by hostiles in two main ways:

- denying them the ability to obtain the information they need from their research because they simply cannot obtain it, or they could but the risk of detection to achieve this is too high
- promoting failure – both of their ability to conduct hostile reconnaissance (they will not be able to get the information, they will be detected) and of the attack itself

These effects can be achieved because in the process of conducting hostile reconnaissance the hostiles are making themselves vulnerable – they are online and at the site looking for and obtaining this vital information.

Protective security can therefore be focussed in the following manner: to *deny* the hostile the opportunity to gain information, to *detect* them when they are conducting their reconnaissance and to *deter* them by promoting failure through messaging and physical demonstration of the effective security. This approach will play on their concerns of failure and detection.

The key to disruption comes from understanding the information hostiles need, and where they are going to have to go to get this and their state of mind. This, in turn, is dependent on understanding the threats in a way that enables prediction of likely attack scenarios.

Understanding the threat

It is important that an organisation understands the threats it faces. Not all threats are applicable to all organisations so it is important that a security department understands what it is defending against.

While an organisation may face a variety of different threats with different attack scenarios, there are likely to be commonalities in information requirements across these. Therefore measures put in place to disrupt hostile reconnaissance can be effective over a wide range of threats.

Given that not all threats are the same, a useful way of understanding those particular to an organisation is to consider the mindset of the hostile.

A hostile's mind-set is determined by Intent, Capability and Culture. By understanding this, together with the assets you are trying to protect, you can understand likely attack scenarios.

Intent	This is what the hostile wants to achieve. Think about their overall aim as this will help identify the effect the hostile wants the particular attack to have
Capability	This is about the resources at the hostile's disposal. Think about equipment, time, personnel, skills and training, financial backing and geographic location
Culture	This is the hostile's personal motivations and appetite for risk

A security manager may not be able to answer every question relating to a hostile's mind-set but by attempting to understand it they can better determine likely attack scenarios, and therefore what information is needed, and where they will go (online, onsite, inside knowledge) to get this.

Security managers should revisit and update these scenarios regularly as their understanding of their threats evolves. As each route is closed to hostiles, the more motivated and those flexible in time and resources may continue to look at alternative ways to achieve their aims, including the use of insiders (those that use their legitimate access to an organisation to cause harm).

Conducting this assessment across all the main threats will enable an organisation to identify commonalities in information requirements. This assessment will enable the security manager to focus their protective security measures, whether cyber, personnel or physical, more effectively to disrupt a range of hostile groups and to be as effective as possible if the threat increases.

The next section will examine the principles of countering hostile reconnaissance.

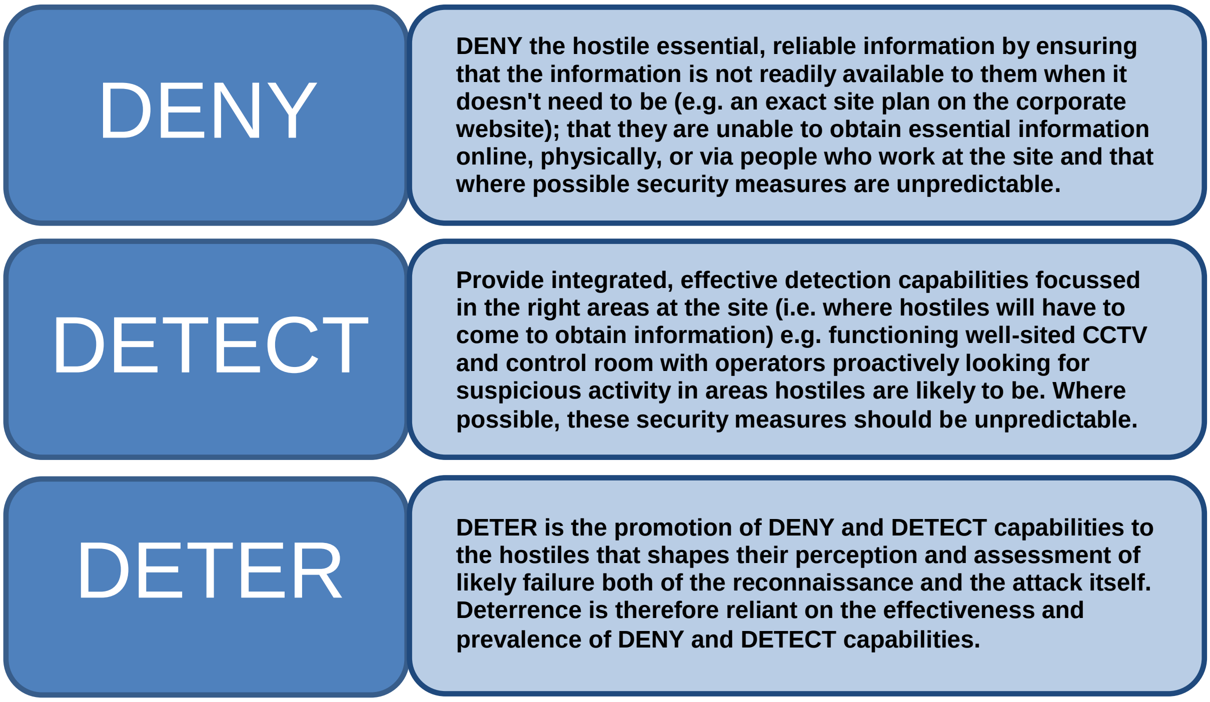
Countering hostile reconnaissance: the principles

Understanding the threat can allow a security manager to determine:

- what information the hostiles will be looking for and why
- where the hostiles will go to obtain this information
- the hostile mindset: how far they will go (effort and resource, motivation and risk appetite) to get the information they need

Once this is understood an organisation can shape its protective security and other resources such as corporate communications and employee behaviours, to help disrupt hostile reconnaissance. This section describes what these principles are, how they work to disrupt hostile reconnaissance and how they can be applied in terms of activties at a site.

CPNI research has shown that there are three principal ways that this can be achieved – **DENY**, **DETECT** and **DETER**:



DENY

DENY the hostile essential, reliable information by ensuring that the information is not readily available to them when it doesn't need to be (e.g. an exact site plan on the corporate website); that they are unable to obtain essential information online, physically, or via people who work at the site and that where possible security measures are unpredictable.

DETECT

Provide integrated, effective detection capabilities focussed in the right areas at the site (i.e. where hostiles will have to come to obtain information) e.g. functioning well-sited CCTV and control room with operators proactively looking for suspicious activity in areas hostiles are likely to be. Where possible, these security measures should be unpredictable.

DETER

DETER is the promotion of DENY and DETECT capabilities to the hostiles that shapes their perception and assessment of likely failure both of the reconnaissance and the attack itself. Deterrence is therefore reliant on the effectiveness and prevalence of DENY and DETECT capabilities.

The diagram on page eight illustrates the relationship between these three key components of disruption and, if done well, the effects of these on the mindset and assessment of the hostile.

DENY them what they need

Denying the hostile the information they need to fulfil their information requirements is the first step an organisation can take in forcing the hostile to either disregard them as a target or ensuring that they have to undertake further, potentially detectable, reconnaissance.

Removing or modifying information from public-facing websites and educating employees on what kind of information hostiles will be looking to harvest from, for example, their social media accounts, is a simple yet efficient means to deny the hostile what they need.

Denying what they need can also mean creating uncertainty and unpredictability about security arrangements at a site. For example, unpredictable timing, type and location of security patrols makes it difficult to determine a pattern of activity that they can exploit with any confidence.

DETECT and the state of mind of the hostile

Detection and the promotion of integrated, effective capabilities, such as vigilant and engaged security officers with timely and appropriate response, can be particularly powerful. This is because hostiles operate with a different mindset to the normal site user. They know they are on site for malicious reasons and they know that they be might behaving in a way that is out of the norm, thereby making them more anxious or paranoid and therefore potentially susceptive to detection.

This natural anxiety can be amplified by communicating and demonstrating the range and effectiveness of the detection capabilities at the site. This is the vital function of deterrence.

DETER - generating and sustaining deterrence

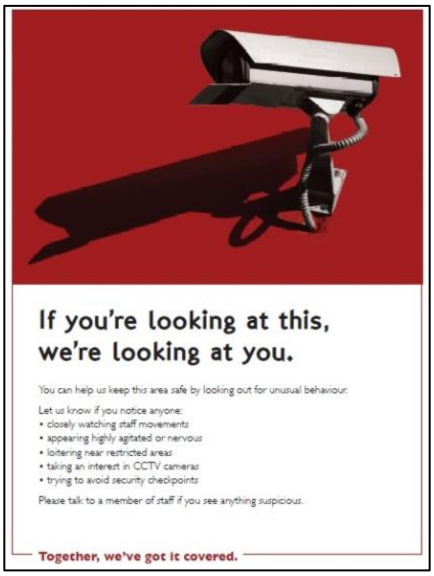
Deterrence is a vital component of disrupting hostile reconnaissance. Deterrence is, for a majority of sites and organisations, the main desired effect of their protective security on hostiles. In many cases it is assumed that because protective security measures are in place they are, by default, deterring. To get the most out of deterrence for a site requires proactive effort by the organisation.

CPNI defines deterrence as: “The intelligent, co-ordinated promotion of protective security provision to the hostile that results in the perception and/or assessment that the reconnaissance or the attack itself will fail.”

This is about **proactively marketing** protective security provision, primarily an organisation’s DETECT and DENY capabilities, to the hostile audience. Hostiles are looking for critical information and evidence about these measures online and at the site to help inform their attack planning.

As such, the fact they are actively conducting information gathering activities (i.e. that they are ‘tuned in’ to information about security measures and state of security at the site) can be used as a way of delivering deterrent messaging to them.

The messages, such as the one illustrated to the right, should convey that these capabilities are in place and that they will be unable to gain access, or have sufficient confidence in the information essential for attack planning without an unacceptable risk of being detected.



If you’re looking at this, we’re looking at you.

You can help us keep this area safe by looking out for unusual behaviour.

Let us know if you notice anyone:
- closely watching staff movements
- appearing highly agitated or nervous
- loitering near restricted areas
- taking an interest in CCTV cameras
- trying to avoid security checkpoints

Please talk to a member of staff if you see anything suspicious.

Together, we’ve got it covered.

The importance and benefits of deterrence

If an organisation does not proactively ‘promote’ its DENY and DETECT capabilities to hostiles then it is missing an opportunity to disrupt hostile reconnaissance. The organisation loses the chance to get the hostile to discount a site as a target at the initial target selection phase (which may be conducted primarily online), or at least prime them to be anxious and concerned about being unable to gain access and be detected when conducting physical reconnaissance.

For example, an organisation may have an excellent employee vigilance and reporting culture, with staff reporting in suspicious activity immediately and security officers officers responding rapidly. This can be hugely deterring to the hostile – it's not just CCTV and security officers they need to worry about spotting them, everyone could be watching.

These effects work for a multitude of protective security capabilities. Of course, this has to be done carefully and needs to be achieved in a way that doesn't give hostiles the information they are looking for.

How to proactively promote DENY and DETECT capabilities to DETER

How an organisation provides its messages and evidence of these capabilities needs to be done carefully and thoughtfully. For example, being considerate of the normal site user and their perceptions of such messages (ideally to be reassuring and informative or to have a neutral effect), and critically, to convey the protective security without giving away detail that could be helpful to hostiles

It is important to see this not just as a one-off requirement. Hostiles will potentially be coming back many times online and at the site, so it is important to keep the 'drumbeat' going in terms of promoting capabilities.

Where possible, use video and pictures – social media is an excellent platform for this – to help provide credible evidence that these capabilities exist and work. For these reasons, *'co-ordinated'* is also an important term in CPNI's definition of deterrence. For example, if an organisation has just had CCTV cameras upgraded, there is a perfect opportunity to put out a news story in the publically-available site magazine, informing about its effectiveness but without giving away too much technical information that would assist the hostile.

However there is an important caveat to the promotion of DENY and DETECT capabilities. **Any promotion of capabilities must be truthful.** If it isn't, the hostile will soon uncover this deceit, with the resulting effect of potentially not believing anything that an organisation has highlighted and potentially even motivating them to continue.

Hostile reconnaissance checklist

Once they have understood the threats that they face and the principles of DENY, DETECT and DETER, organisations can help reduce their vulnerability to online and physical hostile reconnaissance by considering the following six themes:

- secure online presence
- robust entry process
- hostile reconnaissance threat is understood
- strong staff security awareness
- vigilant and professional security
- deterrence strategy

When thinking about these, security managers should ask themselves the questions on the following pages and if they are unable to answer them, they should consult the CPNI or the National Association of Counter Terrorism Security Officers (NaCTSO) websites, or they should speak to their CPNI adviser or Counter Terrorism Security Advisor (CTSA).

Question	Yes/No	What will be the result?
Does your organisation think about the information it puts into the public domain and consider what positive/negative impact this may have on those engaged in hostile reconnaissance?		Your organisation considers and manages what information is available about it in the public domain and this will help deter those carrying out online hostile reconnaissance.
Do your employees understand why they need to be aware of what information they reveal about themselves or their organisation when online?		Your employees consider the impact their digital footprint has on both them and the organisation they work for, thereby making it more difficult for hostiles to harvest information from them.
Does your organisation understand the threat posed by employees inadvertently giving away information or allowing unauthorised access or malicious software onto your systems?		Your organisation has an understanding of how spear phishing (and similar) attacks are conducted and what can be done to mitigate them.

Question	Yes/No	What will be the result?
Do your employees undergo identity and document verification training?		Employees tasked with document verification, whether during pre-employment screening and/or during visitor entry, are vigilant to the threat of fraudulent documentation.
Are your security personnel sufficiently motivated to identify, deter or detect hostile reconnaissance?		Motivated, attentive and observant security personnel that can form a highly-effective deterrent presence and final line of defence where other interventions may have failed.

Question	Yes/No	What will be the result?
Do you understand what hostile reconnaissance is, where it may be conducted at your site and what you can do to deter or detect it?		Potential hostile reconnaissance points are identified and mitigation measures introduced.
Do you make use of deterrence materials such as security posters aimed at hostiles, in and around your site?		Security managers are given the materials and support to carry out a deterrence messaging campaign, resulting in the deterring or detecting of hostiles.

Question	Yes/No	What will be the result?
Have you measured your organisation's security culture?		Your organisation understands its security culture and identifies where and why it might need to change.
Do your employees know why they need to be vigilant in and around their place of work?		Employees display vigilant behaviours in and around the workplace, thereby making them less of a target and more likely to identify those conducting hostile reconnaissance.
Have your employees been educated as to why their security behaviours in the workplace matter?		Employees display good security behaviours in and around the workplace.
Do your employees know what social engineering looks like and what to do if they think it is happening to them?		Employees recognise social engineering approaches and respond appropriately.
Do your employees understand why they need to be aware of what information they reveal about themselves or their organisations online?		Your employees consider the impact their digital footprint has on both them and the organisation they work for, thereby making it more difficult for hostiles to harvest information from them.
Do your organisation's line managers understand the role they have to play in security?		Managers consider security while making day-to-day business decisions and ensure their teams are kept up-to-date on security matters.

Question	Yes/No	What will be the result?
Does your security department understand the threats it faces?		Security personnel understand the threats posed to their organisation and are motivated to identify and disrupt hostile reconnaissance.
Do your security personnel display a professional-looking presence, profile and posture?		Security officers are motivated to identify and disrupt hostile reconnaissance.
Have your security personnel received training in detecting suspicious behaviour and tactical questioning?		Security officers can more readily identify hostile reconnaissance and resolve suspicions through questioning.

Do your CCTV operators know what to look for in terms of hostile reconnaissance?		Improved effectiveness of CCTV operators in deterring and detecting hostile reconnaissance.

Question	Yes/No	What will be the result?
Do you make use of deterrence materials in and around your site?		Hostiles are deterred by, or detected as a result of, your deterrence materials.
Are you considering how all the elements of your security and communications assets can be used together when deterring and detecting hostile reconnaissance? Are you intelligently promoting your security measures?		Security managers understand the threat from hostile reconnaissance. Your organisation's security assets are coordinated and utilised to create the maximum effect.

CPNI advice

The CPNI website – www.cpni.gov.uk provides more information on how to deter hostile reconnaissance.

Relevant guidance includes:

Employee Vigilance campaign
Workplace Behaviours campaign
Social Engineering: Understanding the threat
Guard Force Motivation

For more information, please contact your CPNI adviser or CTSA.

Other CPNI products

If the hostile is unable to gather the information they require from their online or on-site reconnaissance, they may attempt to recruit an insider to help achieve their aims.

To help mitigate the threat of insiders, CPNI has produced a range of personnel security guidance products and training based around the following four components:

- personnel security risk assessment
- pre-employment screening
- ongoing personnel security (aftercare)
- security culture

When applied consistently, personnel security measures not only reduce operational vulnerabilities, they can also help build a hugely beneficial security culture at every level of an organisation. Robust personnel security helps organisations to:

- employ reliable people

- minimise the chances of staff becoming unreliable once they have been employed
- detect suspicious behaviour and resolve security concerns once they emerge

Physical security

CPNI has also produced a range of physical security guidance products and training looking at the following areas:

- chemical, biological, radiological
- CCTV
- explosives and ballistics protection
- hostile vehicle mitigation
- lighting and obscuration
- perimeters and access control
- secure destruction of sensitive items
- search and screening
- physical security over IT

Utilisation of and, where appropriate, demonstration of efficient physical security measures will help with countering hostile reconnaissance.

A good starting point to help plan the implementation of security measures is to read CPNI's Guide to Producing Operational Requirements for Security Measures. This lays out a systematic assessment process and has been successfully used in many organisations.