Safe and Protect Kirklees

Keeping Kirklees Safe from Terrorism and Violent Crime

Issue 12: January 2026

General Reminders

- ***Terrorism:*** *Updates and wider guidance on Martyn's Law and other wider counter terrorism advice can be obtained from ProtectUK, where you can also subscribe to update emails. To access this advice and sign up to these emails visit:* ProtectUK. ***Action to consider:*** *We strongly encourage all businesses and community groups to sign up to this platform for easy access to updates and guidance linked to counter terrorism and security.*
- ***Crime and Safety:*** *More information around services in place to support crime and safety concerns within Kirklees can be obtained from* Safer Kirklees and West Yorkshire Police.

Current National Terrorist Threat Level: SUBSTANTIAL

(The Threat Levels are designed to give a broad indication of the likelihood of a terrorist attack. They are also a tool for security practitioners working across different sectors and the

police to use in determining what protective security response may be required. Please click the terrorism threat level indicated above to learn more).

Bulletin Content

- Insider Threat
- Competent Person Scheme Update
- Security Culture Tool
- Reducing Permissive Environments in Education
- Other Articles and Information of Interest
- Training and Awareness
- Reporting Concerns
- Contact

Insider Threat

Threats that result from the actions of an employee, former employee, or stakeholder. Insider threats can be intentional or unintentional.

A man has recently been arrested following a British Transport Police investigation into the abuse of access to some Network Rail Wi-Fi services. The man is an employee of Global Reach Technology who provide some Wi-Fi services to Network Rail. He has been arrested on suspicion of offences under the Computer Misuse Act 1990 and offences under the Malicious Communications Act 1988.

Anyone who has, or at one time had, access to confidential or proprietary information can be a threat to organisations. Insiders have knowledge and understanding of internal processes and structures, making it easier for them to cause incidents. As they already have this access, it can also be more difficult to detect incidents. If an insider is actively seeking to harm a business, then they can use login credentials to steal, leak, modify or sabotage data. These actors could be acting on personal motives, or under direction from other malicious parties e.g. extortion attempts.

An unintentional insider threat can be just as damaging. Although there may not be any intent to do harm, employees often make mistakes - they can have their accounts compromised, or they can be socially engineered to perform unintended actions. The below advice can help mitigate the threat from insiders.

- **Implement good hiring policies** Make sure staff are vetted to a suitable degree, this should extend to 3rd party vendors, sub-contractors and other partners.
- **Review dismissal policies** This includes revoking user access to systems before employees are informed that they're being let go, escorting them off premises, and changing any login credentials that they might know of.
- **Principle of Least Privilege** Employees should only have access to data which they need for their role. Reducing the number of privileged accounts means that there are fewer of these higher level accounts to be compromised. With this in mind, it's important to update employee privileges when they change jobs, so they don't retain previous levels of access.
- **Segregation of duties** Although you should reduce the number of privileged staff as outlined above, it's also good practice to make sure that sensitive processes require more than one person to complete them. This can reduce fraud, error, and over reliance on single employees.
- **Monitoring user action** Monitoring and logging work sessions and network performance is a good way to identify abnormal behaviour either intentional or unintentional. Obviously, this can be a sensitive area, and the level to which you will want to do this will depend on your need. Your budget will also define what options are available to you. The NCSC have provided guidance around what exactly technical professionals should be logging.
- **Training and awareness** Implement regular cyber security training and awareness sessions to raise awareness of how employees can protect themselves and others.
- **Building a healthy work environment** A positive work environment which encourages open communication can help to tackle both intentional and unintentional insider threats. Not only will it reduce the likelihood of employees becoming discontented, but staff will be more ready to discuss the security concerns in general if they don't fear reprisal.

Competent Persons Scheme Update

Businesses and organisations are being helped to better prepare for terrorist attacks, upskill their people, and access trusted expertise thanks to new measures being introduced by Counter Terrorism Policing (CTP).

As the lead for countering terrorism threats in the UK, CTP has announced two new initiatives to strengthen the UK's protective security and organisational preparedness – a register of verified specialists and a Level 3, Ofqual-regulated qualification.

Both initiatives address recommendations made by the Manchester Arena Inquiry.

The first is a new national Counter Terrorism Security Specialists Register. From spring 2026, businesses and organisations will be able to access a CTP-endorsed register of qualified specialists who provide protective security and organisational preparedness advice and support.

The second is a separate initiative, a new Ofqual-regulated qualification: Competent Person in the Workplace. This has been designed for security, health and safety, and operational professionals responsible for managing protective measures in their organisation.

Jon Savell, Deputy Assistant Commissioner Specialist Operations, said: “Our aim is to empower organisations to make informed decisions about protective security and preparedness.

“We have listened carefully to industry feedback, which has been very clear: organisations want to be able to access professional and credible advice. These two initiatives respond directly to that. They offer proportionate, practical tools to help venues raise their standards and strengthen protective security, giving organisations the confidence and trusted support they need to protect the public.

“Our overarching goal is to keep the public safe from the threat of terrorism, and providing businesses and organisations with easy access to get the best advice will go a long way to achieving that goal.”

The Register will be delivered via a partnership between the National Counter Terrorism Security Office (NaCTSO) – a specialist unit within CTP – and the National Protective Security Authority-sponsored Register of Security Engineers and Specialists. It will be administered by the Institution of Civil Engineers. Members of the Register are bound by a code of professional conduct.

This will provide:

- access to trusted, competent specialists
- assurance that individuals meet recognised standards
- confidence that members are bound by a professional code of conduct
- a straightforward way to identify qualified counter terrorism protective security support.

If organisations need counter terrorism protective security, preparedness advice, or technical implementation, the Register will offer access to a wide pool of verified expertise across multiple disciplines.

NaCTSO is working with awarding body, SFJ Awards, to develop a new counter terrorism-specific protective security and preparedness qualification.

The Ofqual-regulated qualification is currently being finalised and will formally launch in March 2026 at the Security and Policing event.

This is a Home Office-funded project, created following the Manchester Arena Inquiry report, and will provide organisations with the toolset to understand and mitigate their threat and risks from terrorism.

David Higham, Managing Director of SFJ Awards, says: “Against the backdrop of increasing terror threats, counter terrorism-specific protective security and preparedness are increasingly central to the operational resilience of organisations and employers.

“The Competent Person in the Workplace qualification will provide a structured, Ofqual-regulated pathway to building capabilities in this area, and we are proud to have been appointed as the designated awarding organisation for this qualification which is due to launch soon.

“Home Office and CTP’s direct involvement in designing the course and qualification means that it sets the standard for learning amongst professionals responsible for counter terror measures in their organisations. This will be the only Ofqual regulated CTP and NaCTSO endorsed qualification in the marketplace focused on protecting premises from terrorism.”

(The above article can be found on the Counter Terrorism Policing website for onward sharing as required)

Security Culture Tool

Developing and sustaining a proactive security culture can help you to mitigate against a range of threats that could cause operational, reputation or financial damage to your organisation. It is an essential component of any protective security regime.

If used in the right way, your staff, guard force, contractors, visitors, suppliers and the general public can be a huge force multiplier, at no or low cost, in strengthening your resilience to security threats and reducing your vulnerability to attack.

Effective security culture is seen as a vital part of protective security across industry and Government.Investing in security culture helps establish a workforce that is engaged with,and takes responsibility for, security issues. This is vital in a rapidly changing world where threats and vulnerabilities are evolving; having a workforce that is resilient and can spot and report potential vulnerabilities is crucial to your organisational health. The following considerations form the basis for this security tool.

- **Cumulative Risk:** Poor security behaviours, even if accidental, can add up and lead to accumulation of risk and major security breaches. An effective security culture can help minimise this risk due to more staff demonstrating the right behaviours and practices, stopping bad behaviours from spreading or becoming normalised.

- **Adaptability:** Maintaining your workforce's awareness of the threat, and how their own behaviours open up both themselves and your organisation to vulnerabilities,can help develop a security mindset. With the right security culture initiatives in place, your people are more likely to adapt and respond to evolving threats rather than ignore them.
- **Resilience:** Increased awareness of the threat and engagement with security means that your workforce can spot and report potential vulnerabilities, making your organisation a much harder target. This also enables you to intervene early and prevent a full-scale incident from occurring, increasing your ability to manage the impact of unexpected disruptions.
- **Efficiency:** Security can sometimes be perceived as a blocker to wider business performance. When you have an effective security culture, your workforce understand what is expected of them and how security supports wider business goals. Security becomes second nature, which not only increases the efficiency of your security measures, but of your organisation as a whole.

The NPSA has launched a free self-serve tool for businesses and organisations to help them understand their organisation's security culture and how to enhance it. The new Security Culture Tool is structured around four core components – one interactive workshop and three workforce surveys – each of which helps them to understand a different aspect of their organisation's security culture.

Investing in this security culture means that businesses and organisations can establish a workforce that is engaged with, and takes responsibility for, security issues. This is vital in a rapidly changing world where threats and vulnerabilities are dynamic; having a workforce that is resilient to these changes and can spot and report potential vulnerabilities is crucial to their organisational health.

Further information and access to the tool can be found as follows:

- Security culture landing page
- About the tool
- Direct link to the tool

Reducing Permissive Environments in Education

The updated Prevent Duty Guidance 2023 introduced a new theme of Reducing Permissive Environments.

One way that Prevent seeks to tackle the ideological causes of terrorism is by limiting exposure to radicalising narratives, both online and offline, and to create an environment where radicalising ideologies are challenged and are not permitted to flourish.

Education settings should have measures in place to prevent their facilities being exploited by radicalisers. This includes seeking to ensure that event spaces and IT equipment are not being used to facilitate the spread of extremist narratives which encourage people to participate in or support terrorism. The statutory guidance also stresses the need for schools, colleges and other specified authorities to ensure due diligence in relation to the awarding of Prevent funding or contracts.

Please contact Kirklees Prevent Team for further guidance around Reducing Permissive Environments.

Other Articles and Information of Interest

Below are a number of links to other articles and information which you might find interesting:

- **North East ACT Regional Event** - Counter Terrorism Policing North East are proud to be hosting an Action Counters Terrorism (ACT) Regional event. ACT Regional events are designed to raise awareness of the work police and partners are doing to mitigate the terrorist threat, and signpost attendees to guidance and resources to enhance the protective security and preparedness of your own business/organisation. The event will be delivered by subject matter experts including the National Counter Terrorism Security Office (NaCTSO) and Counter Terrorism Policing (CTP). The event is on the Thursday 26th February 2026, hosted at York Biotech Campus, YO41 1LZ. If you are interested in attending this event, please sign up (please note: signing up does not guarantee a place, you will be sent further details on registration if you are allocated a space once request to attend has been reviewed). A light lunch and refreshments will be provided, and a cafeteria is also available on site (if you have any dietary requirements, please email CTSA.supervision@ctpne.police.uk). You will gain a valuable insight into topics including:
    - Risk Management
    - Counter Terrorism Communications Campaigns
    - ACT in a Box – interactive self-delivery training for businesses of any size
- **Countering the Threat of Sabotage Operations to UK Interests and National Security** - The National Protective Security Agency (NPSA) have released a 12 minute video to give information around countering the threat of sabotage operations to UK interests and national security.

- **Cyber Essentials Supply Chain Playbook** - There have been too many occasions where we've seen first-hand the impact that cyber attacks can have on businesses. Supply chains can provide numerous points that attackers look to exploit, but only 14% of firms are on top of the potential risks faced by their immediate suppliers. Specific actions on securing supply chains using the Cyber Essentials scheme should be a priority for every company. The Cyber Essentials Supply Chain Playbook has been developed with the National Cyber Security Centre to help organisations manage their supply chains more effectively, ensuring their operations are protected every step of the way (*Liz Lloyd, Cyber Security Minister*).
- **Cyber Action Toolkit:** The Cyber Action Toolkit is a free, personalised cyber security solution for sole traders to small organisations recently launched by the National Cyber Security Centre that turns cyber protection into simple, achievable steps for your business. With built-in features that recognise your progress, you can work at your own pace, helping you protect your business's money and reputation from cyber criminals.
- **LinkedIn Forum for Martyns Law** - Nathan Emmerich (personal advisor to Figen Murray) has opened a Martyns Law forum on LinkedIn. The Martyn's Law Forum aims to enhance awareness and collaboration between the security sector and businesses with the Home Office and the Security Industry Authority. The Forum is designed to provide meaningful engagement to share exclusive insights, sector expertise, and for organisations to share examples of best practice. Ultimately, it is designed to make the UK safer and to improve security for the public. Engagements must be constructive and respectful. While the Martyn's Law Forum intends to bring businesses and experts together, it is not a purely marketing opportunity for businesses to promote their products or services.Any organisation or professional with the responsibility to implement requirements under the Terrorism (Protection of Premises) Act 2025 can join this forum.

Training and Awareness

Training:

Various training is available for businesses and community groups to increase their levels of awareness and preparedness to protect themselves and others from the risks of terrorism. The main FREE of charge packages are:

- Action Counters Terrorism (ACT) Training
- See, Check and Notify (SCAN) Training

For more details visit Counter Terrorism Police - Advice for Businesses

Awareness :

- Campaign: Please also consider utilising the National Protective Security Authority Community On Your Side toolkit. This is a toolkit that helps you highlight and assess the security measures your site(s) has in place to protect site users from terrorism style attacks.
- Crime Prevention: Please consider how you can help mitigate against crime and terrorism using the Counter Terrorism Crime Prevention Toolkit.
- Kirklees Protect and Prepare Group Website: For general advice, guidance, templates and updates, as well as a contact form to get in touch with the Protect and Prepare team for Kirklees, please see the Kirklees Martyn's Law (Protect Duty) information sharing web page.
- Kirklees Protect Duty web page: General advice page for the wider public of Kirklees. **Action:** Please share this link on your public channels.

Action to consider: Please consider engaging in training sessions and campaigns highlighted above, as well as others as they become available to increase your own knowledge and awareness, and to improve the safety of people across Kirklees.

Reporting Concerns

Terrorism: If you see anything within your communities and causes concern which you believe may indicate the planning or presence of terrorist activity, please report it.

- If you **do not** believe a threat is imminent, please report (anonymously if necessary) what you have seen to the Anti-Terrorist Hotline: **0800 789 321**
- If you feel that an attack is imminent or there is an immediate threat to life, please contact your local police on **999**

Violent Crime: If your concern is around violent crime and there is an immediate threat to life, property or possessions, please contact **999**. For all other concerns please call **101**.

Contacts

For any queries or issues please email:

emergency.planning@kirklees.gov.uk

E-bulletin Distribution and Sign-ups

Please note, as this is a new circulation, you will receive this in the initial instances via other mailing lists you are signed up to. As we make the transition to building up a stand alone distribution list for this e-bulletin, please can you email your details direct to laura.drew@kirklees.gov.uk to ensure you are added to the stand alone circulation list going forward for when the transition is made to our very own sign-up list. Your details will not be shared any further and will only be used for the purposes of circulation of the Safe and Protect Kirklees e-bulletin

Next Edition

The Safe and Protect Kirklees E-Bulletin is issued on a Quarterly basis.

Issue 13 is due for release in April 2026

Previous editions