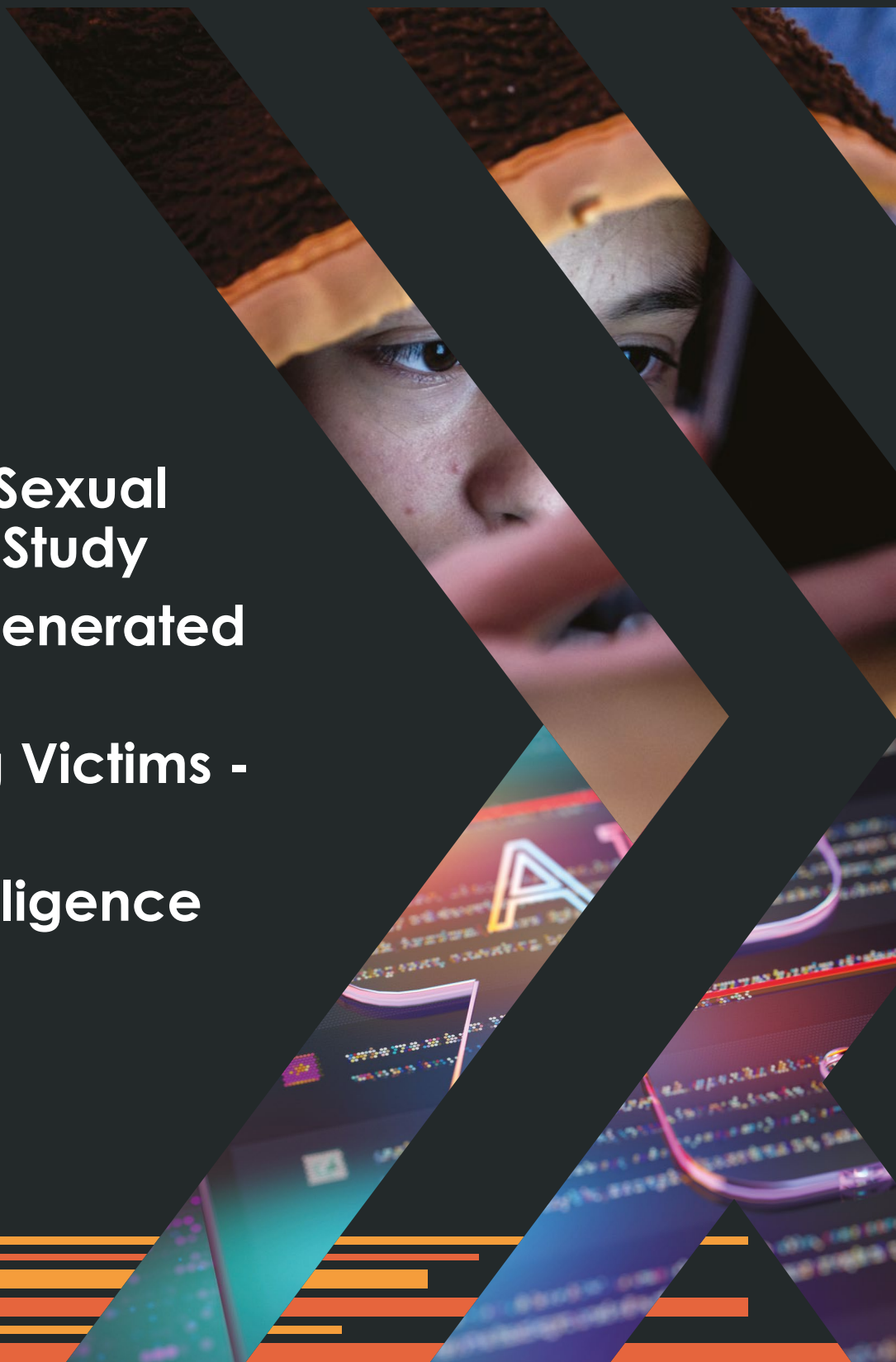
TACKLING ORGANISED

EXPLOITATION

PROGRAMME

Issue 12 | January - March 2025



Inside this issue:

Online Child Sexual Abuse: Case Study

Tackling AI Generated Offences

Safeguarding Victims - St Giles Trust

National Intelligence Awards

#ThankTOEX

Contents

Strategic Update	3
Tackling AI Generated Offences	4
Online Child Sexual Abuse: Case Study	6
Safeguarding Victims - St Giles Trust	7
National Intelligence Awards	8
#ThankTOEX	10
Interesting Reads and Useful Links	11
Upcoming Partnership Events	11

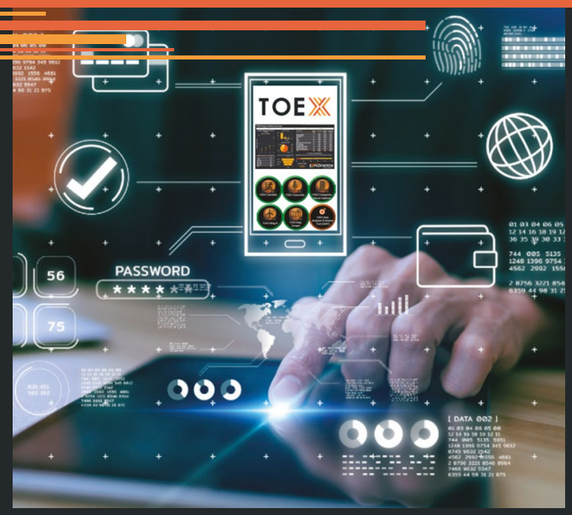
Strategic Update

As we approach the end of the police performance year, the TOEX programme continues to go from strength to strength. Having secured funding for another year and submitted a scalable plan for the governmental spending review thereafter (2026-29), we are able to demonstrate both impressive operational performance and technical delivery that sees us well placed for the future.

The national and international economic challenges being played out in the media are making it clear that all public services will need to realise efficiency savings and prioritise initiatives that offer both good service and value for money. TOEX is well placed to deliver on both counts and the programme SMT has been involved in several national discussions regarding how TOEX will support governmental priorities such as group-based CSE, Violence Against Women & Girls (VAWG) and organised immigration crime.

The National Intelligence Portfolio (NIP) awards hosted by DCC McLaren saw many nominations made for the TOEX category of 'outstanding contribution to disrupting organised exploitation', with some of the nominees highlighted in this edition. The awards served to recognise the contribution made by TOEX and force investigators and we will use some of those investigations as case studies in the future, to showcase how the programme can support frontline investigators in these complex cases.

The upscale of our Capabilities Environment (CE) is progressing well, with over £11 million in saving opportunities realised since the platform became operational in January 2024. The sixth and final app for this financial year will begin testing this month and once approved for release will provide users with the Data Analyser & Review Tool (DART) for the interrogation of digital devices.



A delivery plan has been created for technical workstreams being supported from April, and AI-enabled technology will feature in a number of them. **TOEX ICE (Intelligence Classification Engine)** leverages AI methods to bulk review intelligence reports and identify those that are potentially CSAE but have been incorrectly tagged and require human review. Pervading data quality challenges hinders both service delivery within individual cases and the force's ability to understand/respond to threats. Secondly, **TOEX Scan Assist** is a threat neutral AI-powered workflow that turns any single column of intelligence into a fully interactive analytics dashboard, with i2 mapping, negating the need for forces to build bespoke analytic reporting tools for each threat. Finally, **TOEX Co-Pilot** proposes the modular deployment of a large language model (LLM) which will initially be trained on exploitation thematic data to allow users to "chat" with the interface and ask questions about exploitation offences and investigative opportunities.

Much is happening in the national policing space, and as a key stakeholder, TOEX is pleased to contribute to discussions regarding the new National Centre for VAWG and Public Protection. As TOEX plans for its move to the NPCC, we will remain engaged with this and the wider police reform agenda to ensure we are ready for future challenges.

Detective Chief Superintendent
Kate Thacker KPM
TOEX Programme Director

Tackling AI Generated Offences

By Paddy Pitcaithly,
TOEX Systems Developer

Last month, the Home Secretary revealed plans for the UK to take a global lead in reducing harm by making it illegal to possess, create or distribute AI tools designed to generate CSAM or to possess AI 'paedophile manuals' instructing on how to use AI to generate CSAM. This is augmented by a specific offence of running websites designed for facilitating sharing of CSAM and related advice. The 'Crime and Policing Bill: Child sexual abuse material factsheet' published on 25th February clarified that the focus was criminalising AI models that have been optimised to create CSAM.

While the prevalence of AI CSAM reported by the Internet Watch Foundation (IWF) is currently low, the threat not only to society but to victims whose image is used in training models and to victims targeted by AI imagery blackmail and extortion is significant.

The threat of AI CSAM generation comes in a variety of forms: models can be publicly hosted (designed to have no technical barriers to use) or open-source and available for a user to download and fine-tune offline. Models can be text-to-image (or text-to-video), allowing a user to enter a prompt description that the model uses to generate in an image, or can take an image as input with a pre-defined target output. This latter category includes 'nudify' apps, in which a user can upload an image and have the app 'remove' clothing by generating an image of the subject's body, as well as 'deepfake' or 'face-swap' apps in which a user can convincingly create a pseudo-image by transposing a subject's face onto an existing image. These, as well as de-aging apps, are frequently used to generate CSAM images involving versions of both adult and child celebrities.

The new offence initiated in April 2024 of creating sexually explicit deepfake imagery successfully led to the blocking in the UK of two of the most widely used 'nudify' apps. These apps continue to proliferate though, with hundreds being used to target children, celebrities, and political candidates amongst their victims. The UK's approach is being considered by other jurisdictions, with the US States of California and Minnesota debating bans and initiating legal action against these apps. Their ownership structures are opaque and despite action from payment system operators they remain capable of receiving payment for their service – the most popular such app is reported to receive 3 million visits per month.

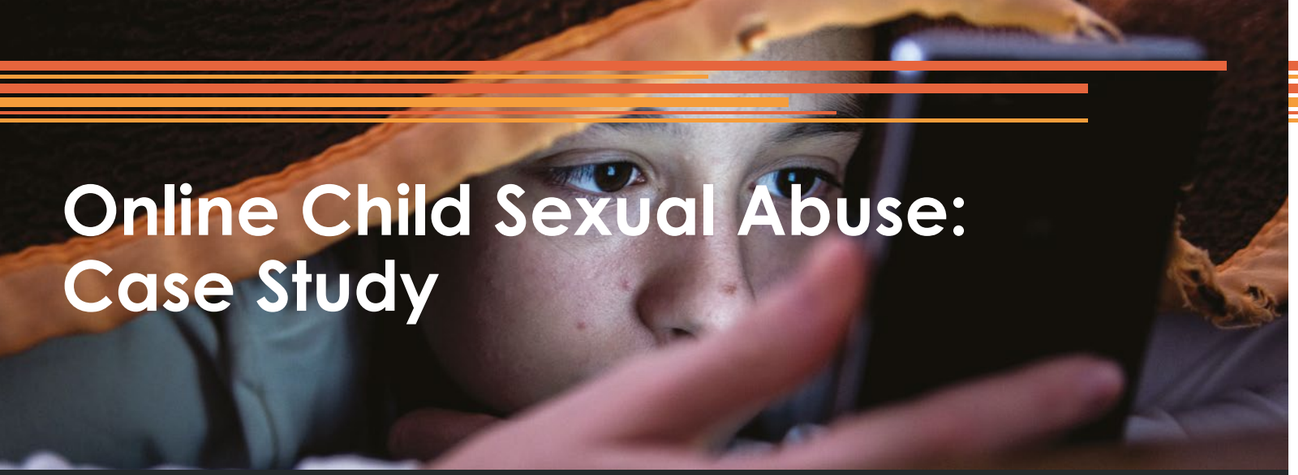
Guardrails on these apps appear to be weak, and despite including warnings that the tools should not be used to create illegal images, the majority of them proudly advertise an 'anything goes' approach. A high-profile incident occurred in Almendralejo, a small town in south-west Spain, in which 15 schoolchildren were sentenced to probation for creating and sharing 'nudified' images of more than 20 girls aged 11 to 17. Another AI 'art' generation app not only allowed users to generate CSAM but left user-generated CSAM on their public website – these images were then indexed by search engines and appeared on Google and Bing searches for the app until reported to the search engines by an investigative journalist. Discord users have shared methods to bypass rudimentary guardrails that have been put in place.

Offline CSAM generation allows users to download models to their local computer. These might be base models that are already capable of generating CSAM, base models for fine-tuning by the user, or models already fine-tuned for CSAM generation. These latter two categories are those that will be illegal to possess. While local fine-tuning requires some technical sophistication, methods exist that allow fine-tuning on very small numbers of images. Some diffusion models have been fine-tuned on datasets composed of images of victims of child abuse – perpetrators then share these models in order to use them offline to generate their own images of these victims.

So what can be done? Research is ongoing regarding identifying which models have been fine-tuned specifically to allow CSAM generation. Unfortunately, popular text-to-image generative base model versions exist that included not only pornography but CSAM in the training data – these models are capable of generating CSAM but this might not be clear to a user. Some degree of memorisation has been identified in fine-tuned models that can be used by law enforcement as an indicative measure of fine-tuning: given a particular prompt, a legal model might produce an output only vaguely related to the prompt while an illegally fine-tuned model might output an image closely related to illegal training images.

The banning of 'paedophile manuals' extends the offence created by Section 69 of the Serious Crime Act 2015 to cover synthetically generated images as well as direct sexual abuse of children. Research by IWF suggests that most advice takes the form of dark web forum comments rather than the sharing of more structured manuals, but some examples of these manuals have been found in circulation.

The development and use of fine-tuned generative AI models perpetuates the abuse and trauma of victims of physical abuse as well as increasing the risk of extortion and the risk of viewers of CSAM seeking direct contact with a child. While the proportion of CSAM identified as AI generated is currently small, the pace of technological development continues to be rapid, with early examples of AI CSAM video content already existing and image quality continuing to improve. Incisive steps to limit the potential misuse of this technology are essential.



Online Child Sexual Abuse: Case Study

TOEX was approached by South Wales Police to assist with an investigation involving the sharing of child sexual abuse material through a Snapchat account.

The account was followed by multiple local school children, who were using it to distribute explicit images, including nude photos of their peers, boyfriends, and girlfriends. Once images were submitted to the account, they were broadcast to the account's followers through its 'Story' feature.

As the account gained popularity, it began to invite more children to become 'friends', significantly increasing the reach of the images. As more children became aware of the account, the explicit content began to draw the attention of concerned parents. Despite being reported to Snapchat multiple times, the account was continuously taken down, only to be re-established under various new versions. In total, investigators found at least 15 variations of the same account.

The TOEX Response

The primary objective for TOEX was to trace the children impacted by the Snapchat account as well as their peers, in a bid to identify the offenders behind these accounts. The team were also tasked with looking at whether there were any cross-border issues, as a similar account had been reported in the Dyfed-Powys police force area.

Using police data and analytical software, TOEX conducted a thorough network analysis, mapping the relationships between the impacted children, their schools, associates, and any related intelligence, allowing the team to identify patterns and pinpoint key individuals involved.

As a result of the detailed analysis, TOEX identified two males for further investigation regarding the distribution of child sexual abuse material. One of the offenders was arrested in connection with malicious communications and blackmail offences and remains on police bail, pending further enquiries.

The investigation remains ongoing in order to identify further offenders and/or criminal activity.

The officer in the case commented

> **"This is amazing to see it like this on paper with the links rather than trying to trawl through a large number of occurrences. Thanks again, saved me and [Officer] a lot of time and identified someone that we had missed also."**

The case highlights the ongoing challenges posed by social media platforms in cases of online exploitation and the importance of a collaborative, data-driven approach to tackling these threats. By piecing together intelligence and conducting an in-depth analysis, TOEX was able to disrupt harmful online content, preventing further children's involvement, and contributing to broader efforts to address child exploitation online.

Safeguarding Victims - St Giles Trust

The St Giles Trust supports and assists individuals affected by various issues, including homelessness, long-term unemployment, offending, addiction, severe poverty, gang involvement, and victims of modern slavery and human trafficking. Read how they're safeguarding victims in the article below:

At St Giles Trust, we are committed to tackling criminal exploitation including child criminal exploitation (CCE) and safeguarding those at risk. Our specialist interventions focus on early identification, protection, and diversion, working closely with communities, professionals, and those directly affected.

A key part of our work is supporting people exploited through county lines—young people coerced into working for dangerous drug networks. Our frontline teams provide one-to-one support, helping them disengage safely and rebuild their futures.

The lived-experience of many St Giles staff in tackling criminal exploitation is at the heart of the services we deliver and means that our staff don't just know the theory of exploitation—they've felt the pressure, seen the manipulation, and understand the risks. They can identify warning signs and tactics used by gangs, helping young people spot dangers before it's too late. They can say, "I've been where you are," making their advice and warnings far more impactful than those from someone without that lived experience.

Our staff can speak the same language as the young people they support. They understand the appeal of fast money, status, and belonging that gangs offer, and they can challenge myths—like the idea that gang leaders "care"—with real-life stories of how exploitation actually plays out.

Many exploited people believe there's no way out. Seeing a professional who has escaped a similar situation and built a positive future provides living proof that change is possible. "If they did it, maybe I can too."

CCE thrives on isolation and hopelessness. Our staff offer an alternative—someone who listens, supports, and shows a different path. By intervening early, they can stop young people from being pulled deeper into exploitation.

Alongside direct support, we also deliver targeted prevention work through our SOS+ programme to build resilience in schools and communities. By raising awareness among in educational settings and with parents, carers, and frontline professionals, we help people to identify the early warning signs of grooming and create stronger safety nets for young people.

Through coordinated, multi-agency efforts, we're making a real difference. But there is more to be done. Together, we can continue to disrupt exploitation and empower those most at risk.

Find out more about our work and how you can support us: Home - St Giles

St Giles

Turning a past into a future

National Intelligence Awards

The National Intelligence Conference and Awards were held on 27 and 28 January – to share best practice and learning and celebrate the exceptional work of individuals from across the intelligence community.

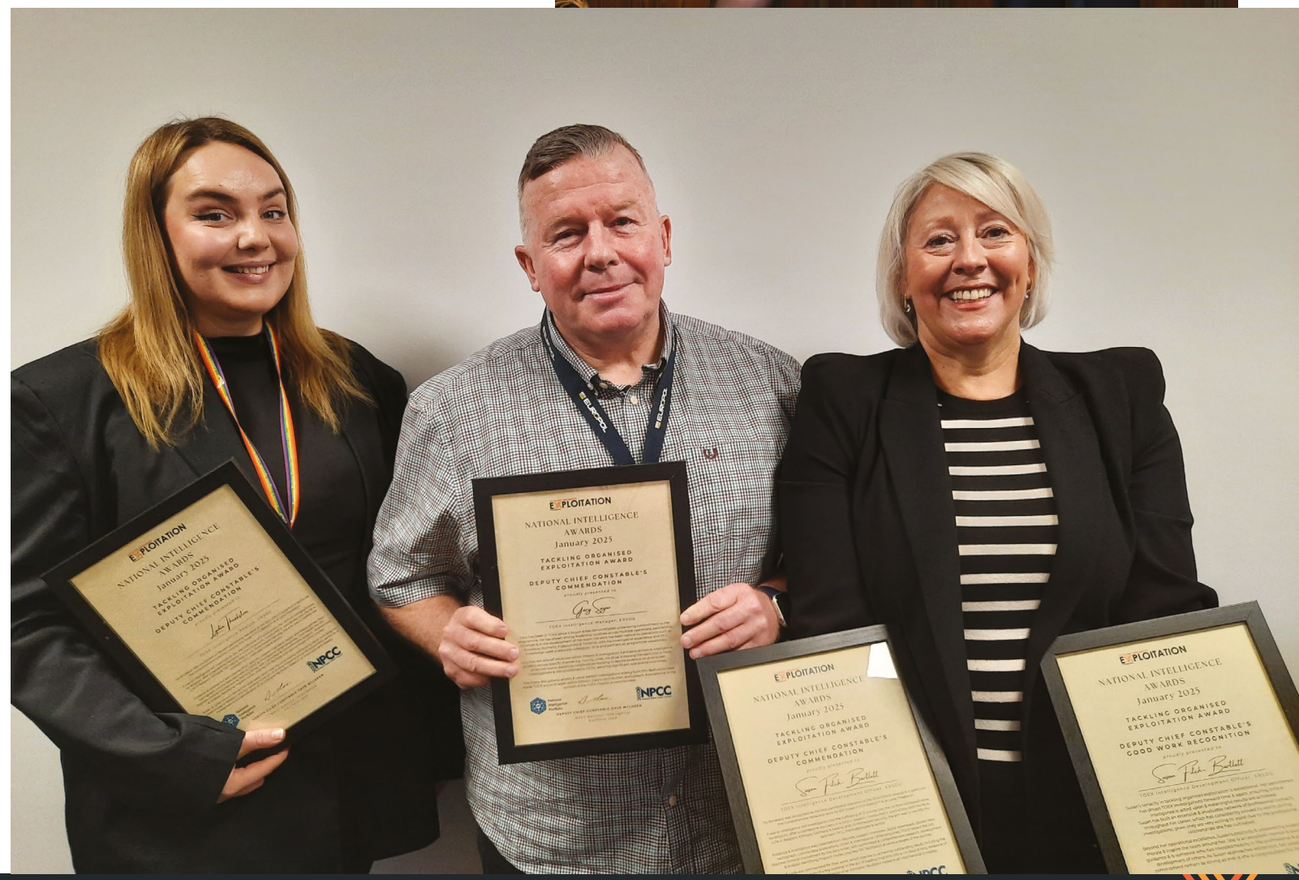
The vision of the National Intelligence Portfolio is to inspire, advocate and support excellence and professionalism within the intelligence community of UK policing and law enforcement partner agencies, in order to protect and serve the public. The aspirations for the portfolio ensures policing is striving to be progressive and innovative, utilising and creating evidence-based methodology, working with partners and academia, to provide the most effective and cutting-edge intelligence capability.

As part of the awards evening, the TOEX award is one of the categories recognised. And this year, we're pleased to announce that the National Technical Team won the award, which was picked up by Detective Inspector Pat Thompson, TOEX Technical Lead, on behalf of the team. The award citation reads:

> **"The National TOEX Technical Team is commended for the unique & ground-breaking delivery of a scalable, cost-effective cloud platform on behalf of the programme & wider policing. The TOEX Capabilities Environment (CE) is the first of its kind to offer a range of secure, assured data tools & capabilities to frontline practitioners in the fight against serious crime.**
>
> **"Already host to five tools, with others to follow this year, the CE is now accessible to the entire TOEX intelligence network & 10 UK Forces, with user numbers increasing rapidly. Significant recognition is shared by industry colleagues & cyber assurance consultants, without whom this work would not have been possible.**
>
> **"The Technical Team is now extending these workstreams to host existing TOEX data analytics products that are delivering force efficiencies in the identification of threat & harm.**
>
> **The team are commended for their tenacity, resilience, innovation & altruism in bringing cutting-edge technology to frontline policing."**

More than 15 nominations were entered for this award and all runners up either received 'Good Work Commendation' or 'Commendation' certificates from the NPCC lead for Intelligence, Deputy Chief Constable Dave McLaren.

Well done to everyone who was nominated!



#ThankTOEX

We are pleased to share that one of our TOEX regional teams has received an award for the work they're doing to support forces to tackle organised exploitation.

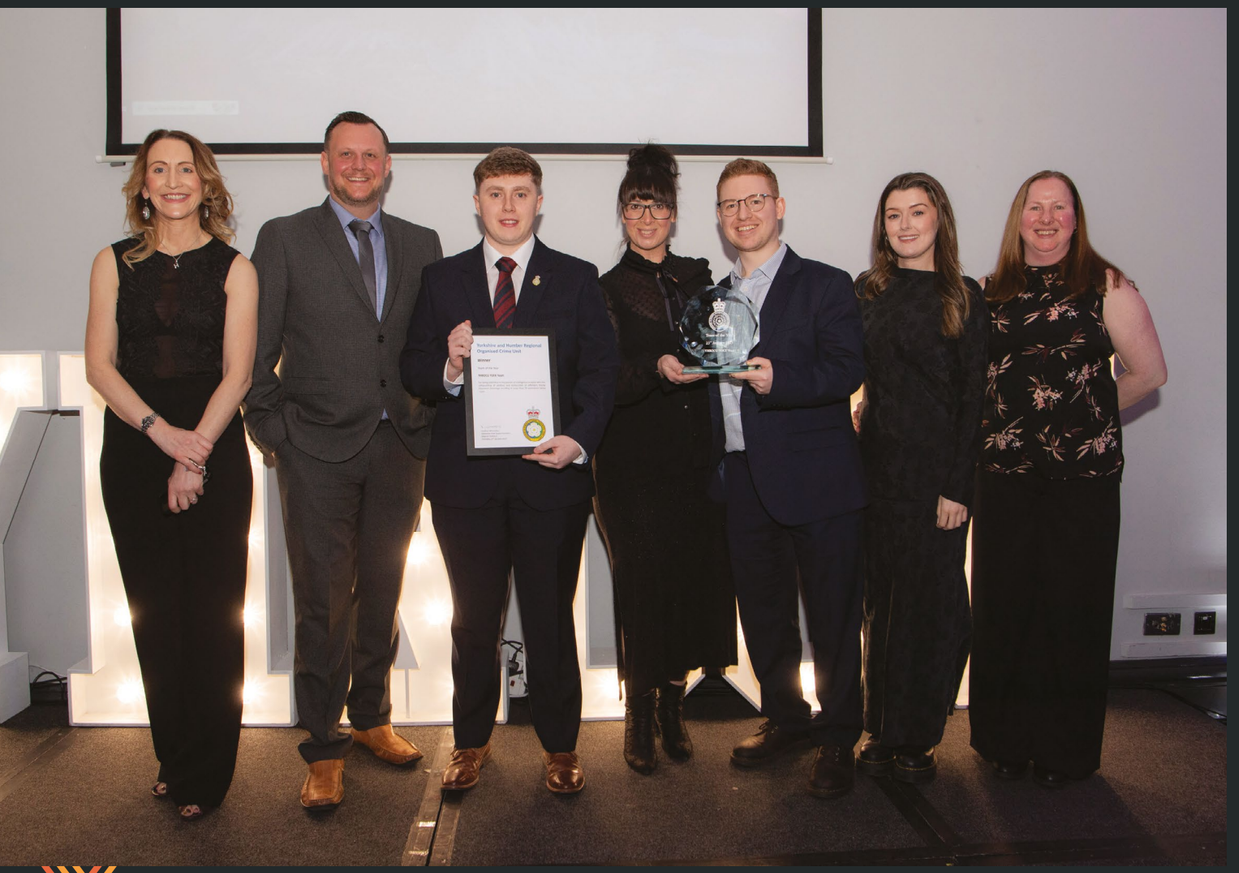
The Yorkshire and Humber team were formally presented 'Team of the Year' at the YHROCU Annual Awards held in January for

> **"being relentless in the pursuit of intelligence to assist with the safeguarding of children and prosecution of offenders..."**

Speaking about the team, colleagues said: "Having built the team from scratch over the last few years, our TOEX team have established themselves as an extremely valuable capability within the YHROCU, supporting our ROCU and our four forces. The team are recognised nationally across the TOEX network as having developed and continuing to develop some of the most complex exploitation investigations and have targeted significant vulnerability."

"The culture within the team is commendable, they have an extremely passionate and innovative work ethic. A peer recently provided praised the team, saying "having worked in and alongside different teams throughout the force, I truly believe TOEX has something very special."

Congratulations to the YHROCU team!



Interesting Reads and Useful Links

The Home Office has published a statement made by the Home Secretary to Parliament outlining the Government's commitment to tackling grooming and child sexual abuse: Tackling child sexual abuse - GOV.UK

WeProtect Global Alliance has released a new film exploring how Artificial Intelligence (AI) is being used to exploit children online: New film exposes AI's role in online child sexual exploitation and calls for urgent global action - WeProtect Global Alliance

The Home Office has confirmed funding for a new centre aimed at enhancing public protection efforts and addressing Violence Against Women and Girls: New Centre for Public Protection to Launch in April | Vulnerability Knowledge and Practice Programme

The Home Office has published a press release announcing new measures to address artificial intelligence (AI) generated child sexual abuse images: Britain's leading the way protecting children from online predators - GOV.UK

The Ministry of Justice has announced legal reforms to support people who have experienced child sexual abuse, in response to IICSA recommendations: New reforms to support victims of child sexual abuse - GOV.UK

NWG Network is inviting child protection professionals to complete a survey about the definitions of various forms of child exploitation: Survey for professionals on the definitions of various forms of child exploitation - NWG Network

Upcoming Partnership Events

- **Data Protection Conference - Tuesday 29 April 2025:**
  Data Protection Conference - Westminster Insight
- **The Supporting Women in Policing Conference 2025 – Tuesday 29 April 2025:**
  www.governmentevents.co.uk/event/the-supporting-women-in-policing-conference/

Contact Us

	Website	**www.toexprogramme.co.uk**
	X (Twitter)	**twitter.com/TOEXProgramme**
	LinkedIn	**www.linkedin.com/company/tackling-organised-exploitation-programme**
	YouTube	**TOEX Programme**

TACKLING ORGANISED
EXPLOITATION
PROGRAMME