

CREATING A SAFER ONLINE ENVIRONMENT: THE LIMITS OF THE POLICE ROLE

Report of the 21st Oxford Policing Policy Forum
held 15 May 2026

By Suleman Lazarus, Michael Skidmore

Edited by Blair Gibbs

THE
POLICE
FOUNDATION

The UK's policing think tank



THE OXFORD POLICING POLICY FORUM

The Oxford Policing Policy Forum (OPPF) is a joint initiative between the Police Foundation, the Centre for Criminology at the University of Oxford, and Thames Valley Police. Established in 2006, the Forum brings together police leaders, policy experts, officials, academics and other stakeholders for discussions about strategic policing and crime issues, held under the Chatham House Rule.

The 21st OPPF was held on 15 May 2026 and the theme was 'online safety and harm'. The Forum followed on from the 20th OPPF, held a year earlier, which examined the government's wider programme of police reform.

Attendees this year agreed that online harm and the police ability to respond to it presents as one of the clearest tests of that reform agenda. It cuts across forces. It cuts across agencies. And it does not fit neatly into the geographic model on which policing has traditionally been built.

This report offers a thematic account of the presentations and discussion held across two sessions. The first session examined the operational challenge posed by online crime. The second examined the response of police, industry and regulators.

Background

Online offending and harm continue to grow in scale and severity. This trend is especially pronounced in online child sexual abuse. The National Crime Agency have estimated that 840,000 individuals now present a risk to children in the United Kingdom. That is around 1.5% of the population. Referrals from the National Center for Missing and Exploited Children (NCMEC) have surged to 92,000 a year. That is four times higher than only a few years ago. Each month, police arrest around 1,000 people and safeguard around 1,200 children in connection with online child sexual abuse.

A wider set of online harms has emerged, often affecting young people. These include sextortion, online radicalisation, self-harm and suicide facilitation, and a loosely defined category of violence facilitated by individuals capable of mass casualty harm. Online violence against women and girls (VAWG) now accounts for one in five of all recorded crime.

None of this sits comfortably within a police system still organised around place and around offences in the public realm. The Forum asked what police reform, and in particular the emerging plans for a 'National Police Service', could do to close that gap.

A changing and escalating threat

Participants described an escalating pattern of online child sexual abuse (CSA). Victims are getting younger. Material is becoming more extreme. Offending is also changing in character. Online communities are forming, often made up of boys targeting girls, motivated less by sexual interest and more by nihilism and a desire for power. A growing number of young people are committing serious offences themselves, often targeting other young people. Sites that encourage or enable suicide were raised as a particularly stark example of diversifying online harms. An estimated 112 suicides in the UK have been linked to so-called suicide kits despatched from online suppliers.

Online offending motivated by financial gain is also impacting the public. Sextortion, perpetrated for profit, was highlighted as a fast-growing and highly damaging form of offending, especially for young victims, and in some cases driving victims to suicide. Cybercrime, particularly ransomware, is increasingly committed by domestic offenders using malware that is freely available online. Some offenders were described as poly online offenders, meaning they can be engaged in multiple online offending behaviours at any one time.

Participants located the underlying cause less in individual pathology and more in platform design. The internet brings offenders and targets (including

children) into contact at scale. This is treated as a foreseeable consequence of how platforms are built, not an accident of poor design. Weak age assurance and largely unrestricted access compound the problem. It was argued that technology companies should do far more to self-police their own customer base and could achieve significantly better outcomes in addressing these harms. However, some perceived that large technology providers had chosen not to.

An online harm in focus: Violence Fascinated Individuals

Violence Fascinated Individuals (VFIs) were discussed as an emerging and poorly understood area of risk. There is no agreed definition. Broadly, it describes individuals not motivated by a coherent ideology who nonetheless pose a risk of mass casualty harm, of the kind seen in the Southport attack in 2024. Around 60% of those identified are boys aged 12 to 16.

Risk factors are eclectic and include personality disorders, misogynistic behaviour, and exposure to extremely violent content. It is usually a combination of factors. The Southport Inquiry identified exposure to degrading, violent and misogynistic material online as a causal factor in the perpetrator's behaviour. The Southport case was cited as a reminder of the risk of treating the manosphere purely as an extremism issue, raising broader questions about how extremism should be defined in relation to VAWG and gender inequality.

Most of these behaviours are lawful in isolation; however, in combination, they produce risk. This creates a significant gap. There is no criminal justice mechanism to intervene, and no equivalent to the Prevent programme used in the prevention of terrorism. Participants identified several specific challenges. Precursor behaviours are usually legally ambiguous and do not meet a criminal threshold. No dedicated intervention exists to manage the risk once identified. Any response needs to be threat-agnostic, since the specific manifestation is likely to change over time. The absence of a settled definition makes it hard to measure the scale of the problem. The issue crosses national borders and multiple online platforms. Law enforcement do not view it as a problem on its own.

VFIs were repeatedly offered as a useful test case for the wider reform programme, a way of stress testing new systems against a genuinely novel threat.

Barriers facing the police and partner services

Detection remains difficult. Many victims do not report what has happened to them. The willingness and capacity of technology firms to share information with law enforcement is highly variable. The full encryption of some devices creates a barrier to evidence collection, and the introduction of end-to-end encryption on some communications apps has already reduced the flow of online CSA referrals from NCMEC to the police. There are some social media platforms that now employ fewer moderators, and as a consequence, provide lower-quality referrals, and others that provide little or no information to law enforcement.

Offending behaviour is also shifting. Fewer offenders now use the dark web. This is not because it has become harder to access, but because it has become unnecessary. Offenders can hide in plain sight on the open web using encryption.

Adoption of artificial intelligence (AI) was seen as offering the police real potential to improve investigative efficiency by processing large datasets and supporting intelligence assessments. However, there is a clear need for safe testing environments before deployment. Participants agreed that a genuinely multi agency architecture is needed, including stalking intervention programmes and earlier action to prevent escalation.

Sentencing was also raised as a weakness. Around 80% of those convicted of online CSA offences (including child sexual abuse material offences or CSAM) do not receive a custodial sentence. Some go on to offend again, sometimes in person, making recidivism a persistent management challenge.

Frontline strain featured heavily in discussion. Operation Soteria led to some police teams becoming overwhelmed, with survivors not always receiving the response they were promised. The cost of monitoring a growing sex offender register was raised as a further pressure, requiring dedicated levers to prioritise risk of harm and prevent reoffending.

One attendee cautioned against treating online offending as disembodied problem beyond the reach of the police; these are real people, using real servers, hosted by real, sometimes deliberately unaccountable, providers, all of which remain legitimate targets for police action here in the UK.

Support exists for victims and their families, but convincing some victims that they are being exploited

remains difficult, particularly where offending communities present themselves as friends. Even with support in place, victims can go on to suffer serious negative health impacts, or even to take their own lives.

Failures across the victim journey were described in stark terms. In one case, police retained a victim's phone for 18 months, yet investigators couldn't access the accounts they needed. The victim's father later succeeded where the police had not. Technology firms have in some cases been fined years after an investigation began, described by one participant as a slap in the face for victims. Reluctance to treat encouraging or assisting suicide as an offence in its own right was also raised.

Services to victims could be enhanced by improved recording and assessment tools to ensure reports are accurately disseminated and the right resources are targeted to where they are needed. International forums such as WeProtect were welcomed as valuable spaces for shared learning, but several participants questioned how effectively that learning currently translates into improved outcomes for victims at the domestic level. Meaningful engagement with victims, survivors and support charities remains limited. In the same vein, civil society organisations doing much of this support work locally with victims remain underfunded.

Beyond location: the limits of policing's geography

Participants argued that online crime challenges some of the basic assumptions built into policing. Police responses are still organised around place, described by one attendee as 'location fixation', which struggles to accommodate online crime that seamlessly crosses jurisdictional borders. Fraud has a single national reporting route for victims, but no equivalent exists to coordinate responses to other online harms such as VAWG offences, even though many victims have now learned to contact Report Fraud by default.

A second challenge concerns definition, with legal frameworks struggling to keep pace with online crime and harm that are continuously evolving. Even when it is unclear whether a criminal offence has occurred, some participants argued that police should still have a role in addressing behaviour that is 'lawful but awful'.

A third and more fundamental challenge is what one participant called policing's real-world bias. Offending increasingly blurs any distinction between online and offline behaviour. But police systems continue to treat

them separately. This affects prevention as much as response. People report online harms to a policing system not well designed to receive them. Several participants suggested that police reform offers a genuine opportunity to redesign, or rewire, the system around this reality, and to build that service capability once at the centre.

Making the case for prevention

The scale of online harm led several participants to argue that current policies lean too heavily on law enforcement and call for a greater focus on prevention. Police were described as ‘beleaguered’ professionals, overwhelmed by a surging demand from online crime. Moreover, many felt that on their own, the police are unable to provide the solution, and that other public sector interventions are needed for ‘moving the dial’ on the current scale of offending and harm.

Participants called for sustainable alternatives, including more offender programmes delivered in the community and stronger education programmes in schools, taking inspiration from the evidence-led prevention initiatives that have been in decline since the 1990s. Key organisations such as the Youth Justice Board need to take more responsibility for children involved in online harm, whether as victims or as offenders. To illustrate, violent pornography consumption was highlighted as widespread and largely unaddressed by policy. Evidence on deviance and crime suggests that exposure before the age of 15 carries a higher risk of entrenched harmful behaviour later on.

Several participants argued that exposure to online material creates its own momentum. It lowers the barrier to offending and draws people in. Over time, this can produce a cycle of habituation towards more extreme content, including CSAM. Individuals become fixated. Early police engagement and diversion, and industry action on reducing access to harmful content, were seen as essential responses.

A key question raised by participants was who ‘owns’ prevention? While it is clear who owns investigation, it is far less clear who owns crime prevention overall, online or offline, or who is ultimately accountable for coordinating it. The current approach is fragmented, with different parts of policing engaging separately, and sometimes inconsistently, with major technology companies on overlapping issues. The forthcoming police reforms were not expected to resolve this, not least because doing so would require dedicated funding.

Within serious and organised crime, the NCA and Home Office already lead on prevention, but participants noted that this strand of work remains comparatively underfunded, reflecting a political preference for visible enforcement over prevention. Furthermore, the NCA are responsible for tackling a serious and organised crime, however many online offences that are serious may not be ‘organised’, so fall outside of its reach, leaving many online harms unaddressed.

The Online Safety Act was discussed, three years after Ofcom gained its powers. Participants argued that safety by design has, in practice, focused too much on content and individual offences and not enough on platform design itself. A recently launched industry code of practice was cited as a step in the right direction, though several participants insisted that any restriction or sanction will achieve little unless it reaches the underlying design and operation of platforms.

Public systems not built for online harms

Participants noted that online crime is not a new problem for policing. They referenced Operation Orr in the late 1990s. Even so, it continues to be treated as novel rather than core business. No one within the National Police Chiefs’ Council (NPCC) held clear responsibility for the Online Safety Act, a gap seen as symptomatic of a wider institutional struggle to grasp the issues.

A communication challenge was raised. Evidence of the endemic scale of online crime continues to struggle to register with government decision-makers. Many people with real influence over policy are not thinking about online harm in any depth. The online environment does not map cleanly onto familiar public and private sector categories. The economic argument was suggested as key to resetting priorities, particularly given the current government’s emphasis on economic growth. This means going beyond the comparatively easy task of costing interventions, to capturing the harder-to-quantify social cost of victimisation over time.

A genuinely threat-agnostic response was called for across this whole area. Several attendees argued that any strategic risk assessment needs to start with a clear picture of the threat, and a practical roadmap for change. The scale of the challenge risks leaving everyone unsure where to begin. A whole-of-society response was seen as necessary, but not, on its own, specific enough to act on.

Some believed that a new National Police Service could strengthen the response to online harm. However, it could also lead to a significant increase in arrests and demand that could overwhelm frontline services. It was suggested that law enforcement is often not the right lever at all. Industry holds more powerful tools to design harm out of its own products, as has been the case in other sectors over the last few decades in response to newly emerging crime patterns. The underlying question, participants agreed, is whether this should be treated principally as a law enforcement problem in the first place.

Industry and regulation: a race with unequal starting points

Tackling online crime effectively requires an ecosystem approach, targeting moderators and administrators of illegal sites as well as their hosting providers. Principles drawn from Routine Activity Theory and Situational Crime Prevention were cited as directly applicable to online spaces.

Undercover online investigators can be dismissed as a drop in the ocean, given the scale of the problem. Participants pushed back on this framing. For the individual child concerned, that intervention is the whole outcome. Targeting the most prolific offenders was similarly defended as producing a disproportionate reduction in harm, even if it cannot resolve the problem at scale.

Industry was described as neither nefarious nor unwilling to help, but currently uncoordinated and under-delivering. The claim that companies want to do good was challenged by some who argued that companies are primarily motivated by profit and, in some cases, would rather not engage with the issue at all. Underreporting was flagged as a problem at every level, and leaving Ofcom – the regulator of the Online Safety Act – to manage this alone was seen as inadequate.

Ofcom set out its role, covering the protection of children from abuse and exposure to pornography, tackling VAWG through better detection and removal of image-based abuse, and addressing online extremism. Some companies have invested seriously in this area. However, overall, the industry response has not matched the scale of the challenge, and current incentives are misaligned, making regulation an essential lever.

Several structural challenges facing regulators were identified. Technology is moving far faster than regulation. A significant asymmetry exists between

regulators and platforms in both technical expertise and resources. The regulatory task spans around 100,000 companies, ranging from the world's largest platforms to tiny operators capable of significant harm. And prioritisation is politically difficult, since deprioritising any single harm rarely feels acceptable.

Industry representatives argued that police are not yet exhausting the channels already available to them, including opportunities for platform-specific officer training and closer knowledge sharing. Technology companies can analyse platform signals and support individual investigations, but do not see it as their role to manage the wider strategic problem. A single shared forum for industry and law enforcement was proposed as a practical next step to improve trust, mutual understanding and coordination.

Safety by design and its obstacles

Participants argued that technology companies need to take responsibility for the technological features within their control. Safety by design was widely supported in principle, but participants were candid about the obstacles to delivering it. These include technological limits, as well as political and cultural resistance. Taking on powerful corporate actors who frame themselves around free speech carries real risk, including the risk that platforms mobilise their own users against reform.

Several participants argued for reframing how misuse is understood. What gets labelled 'misuse' is often simply ordinary use of a feature that happens to enable harm. On this view, companies release technology with certain functionalities and then leave police and regulators to manage the consequences. The focus, it was argued, should not only go to individual bad actors, but also to the underlying question of what 'ordinary' use of a given technology can actually enable.

A product safety analogy was offered, drawing on toys and seatbelts. Products should be tested for safety before reaching the market. A hierarchy of control approach was proposed. Design out the risk wherever possible. Where that is not possible, mitigate it. Where a company can demonstrate it has gone through this process properly, the resulting product should be materially safer.

A key area of discussion was the proposed social media ban for under 16s. Australia's provides an emerging test case. Approximately 500,000 accounts have been closed, however it is estimated that over 60% of

children's accounts remain active. Even so, the policy was credited with shifting public discourse, drawing comparisons with the smoking ban, and with bringing some parents closer to their children's online lives.

A road safety analogy was used to frame the underlying debate. Car manufacturers were once allowed to make unsafe products, until sustained pressure forced safer design. A narrow focus only on dangerous drivers, it was argued, distracts from the inherent risks in driving. In the same way, in light of the challenges to mobilise the technology sector to make the internet safer, a social media ban is analogous to keeping children indoors rather than striving to make the roads safer for their use. Some participants favoured banning specific high-risk functionalities, such as live streaming, rather than banning young people from platforms altogether, alongside a wellbeing-by-design approach to algorithm design. Others argued that an outright ban, while blunt, remains justified given the practical difficulty of banning individual features and the genuine harm it would cause to the underlying business model of affected platforms, notwithstanding obvious workarounds such as virtual private networks (VPNs).

A clear risk was also acknowledged. Larger platforms are already investing in safety technology, even if not at the pace and scale that policing would like. But if regulation, or any ban, does not apply consistently across the sector, and is not assertively enforced, then users displaced from major platforms may simply move to smaller, less responsible ones.

Funding the response

The Home Office was reported as reluctant to keep creating new offences, preferring instead for the Department for Science, Innovation and Technology to lead regulation in this space. Who is ultimately on the hook for prevention remains unresolved.

One proposal discussed was an online safety levy, mirroring the existing economic crime and money laundering levy, requiring well-resourced technology companies to help fund public responses to online harm. This was described as a more fundamental shift than incremental regulatory reform, rooted in a 'polluter pays' logic already applied to other industries.

A related tension concerned where any new investment should go: for example, extra resources for police to respond to victims, or more investment in preventions initiatives such as education for children at risk of victimisation. Several participants argued that

responsibility should not fall on children at all, which brings the focus firmly back onto technology companies.

Participants also noted a structural risk within current reporting duties. Funding should flow to where demand is greatest, but mandatory reporting requirements for CSA, through mechanisms such as NCMEC, are already generating more referrals than police can process. Extending equivalent mandatory reporting across all online harm categories would multiply that problem rather than solve it.

Conclusion

Online safety and harm pose a distinct test for the government's wider reform programme and for the role of the State in keeping citizens safe in a world dominated by technology. It cuts across the geographic model still embedded in day-to-day policing. It cuts across the boundary between online and offline behaviour that offenders no longer observe. And it exposes real gaps in ownership, funding and capability, from VAWG and Violence Fascinated Individuals to suicide facilitation sites and to the pace of technological change and consumer behaviours.

Participants were clear that policing alone cannot resolve this problem. Enforcement remains necessary, but the underlying solution depends on a step-change from industry, via safer product design and closer, active engagement with law enforcement, sustained investment in prevention, and a funding model, potentially including a dedicated levy, that reflects where responsibility for safety online actually sits.

As the government's wider reform programme takes shape, several messages stood out. Treat online harm as a genuine test case for reform, not an afterthought applied to existing structures. Resolve, explicitly, who owns prevention of harm in the online realm, since ownership currently sits nowhere in particular. Push responsibility for safer design upstream onto industry, backed by real enforcement and, where necessary, new funding mechanisms. Anticipate the frontline consequences of a new strategy before it reaches officers already stretched thin. And build a threat-agnostic architecture that can respond to online harms that will keep changing shape, long after the structural changes proposed by the police reform agenda are implemented.



THE
POLICE
FOUNDATION
The UK's policing think tank



21st Oxford Policing Policy Forum

Friday 15th May 2026 from 09:00 – 14:00

All Soul's College, University of Oxford

The Oxford Policing Policy Forum is a joint initiative by the Police Foundation, the Centre for Criminology at Oxford University and Thames Valley Police. First launched in 2006, the Forum provides an opportunity for a wide range of invited stakeholders to discuss the important policing issues of the day, under the Chatham House rule. This provides a rare opportunity for senior decision makers to reflect deeply on key issues in policing. A summary report is published by the Foundation and participation is by invitation-only.

CREATING A SAFER ONLINE ENVIRONMENT: THE LIMITS OF THE POLICE ROLE

The 20th Oxford Policing Policy Forum is on the theme of policing's role in creating a safer online environment. As more of our economic and social life shifts online, debate continues over how to protect vulnerable people from harmful content, the emerging risks that proliferate in the internet environment, and the effectiveness of the new Online Safety Act.

With renewed concerns in recent months about the role of social media platforms and new Artificial Intelligence (AI) tools and ongoing discussion about the responsibilities of regulators and industry, the forum has invited a range of academics, senior police leaders, policymakers and private sector representatives. The forum is designed to consider the scale of the challenge and then debate some of the potential solutions.

Drawing on operational experience and the insight of researchers and practitioners, the forum will examine the historical parallels for addressing the safety challenges that new domains present. In the second part, we will explore the emerging policy and regulatory responses to safeguard citizens in the online realm.

In addition to concrete examples from the current operational environment, the forum allows for open discussion about policing's concerns about the role played by industry and others in creating public safety, and how we should collectively respond to future trends and potential societal and market developments, in order that policy-makers can address them.

Focus for the session

Given the breadth of the topic this year, we have curated the event so that online harms around violence against women and girls, online extremism, and child sexual abuse material are the focus. The Foundation is engaged in other projects relating to fraud, addiction and organised crime.

Pre-reading

Pre-reading for delegates before the event includes:

- The latest National Threat Assessment from the NCA, and the speech given by Graeme Biggar in March 2026;
- An explainer by the Online Safety Act Network of the enforcement approach of Ofcom under the Online Safety Act, including links to guidance and current enforcement tracker.
- The strategic assessment published by the National Centre for Violence Against Women and Girls and Public Protection.
- Ofcom's rules on age-verification for online providers, and their blog from January on 'age-gates' and how these work, and the Online Safety Act itself.

Sponsorship

Police Foundation events are made possible by the support provided by a range of partners including BT, Accenture, Mark43, Forensic Analytics, Palantir and Zencity. All funding for the Foundation and our projects is published on our website.



Agenda

09:00 – 09:30	Arrivals and networking Tea and coffee to be served
09:30 – 09:40	Welcome and brief attendee introductions Professor Ian Loader , Professor of Criminology at the University of Oxford and Director of the Centre for Criminology
09:40 – 11:00	Session 1: Operational challenges of the online realm Graeme Biggar , Director General, National Crime Agency Helen Millichap , Deputy Assistant Commissioner and Director, National Centre for VAWG & Public Protection Paul Court , Deputy Chief Constable, Sussex Police and NPCC Lead for Violence Fixated Individuals, followed by contributions from Maggie Blyth , and Helen King . Discussion chaired by Professor Ian Loader
11:00 – 11:30	Tea and coffee break
11:30 – 13:00	Session 2: The role of the police, industry and regulators in improving online safety Alex Murray , Director of Police.AI Dr. John Higham , Online Safety Policy Director, Ofcom Discussion chaired by Chief Constable Jason Hogg , Thames Valley Police
13:00 – 14:00	Buffet lunch and networking
14:00	Close of event

Chatham House Rule

Under the Chatham House Rule participants can quote and use ideas and information gained during discussions but cannot identify, either explicitly or implicitly, the source of any information or comment, or attribute any quotes to individual participants.

The Police Foundation will compile and publish a short report on key themes emerging from the discussions.

Speaker Biographies



Professor Ian Loader

Professor of Criminology at the University of Oxford and Director of the Centre for Criminology

Ian Loader is Professor of Criminology and Professorial Fellow of All Souls College. He is

also an Honorary Professorial Fellow in the School of Social and Political Sciences at the University of Melbourne.

Ian is a Fellow of British Academy and the Royal Society for the Arts.

Ian is the author of numerous books, edited collections, theoretical and empirical papers, and works of public engagement on policing; private security; public sensibilities towards crime and justice; penal policy and culture; crime control and political ideologies, and the democratic purposes of criminology.

Ian's current work focuses of two projects, both of which are coalescing around aspects of environmental harm. He has recently completed fieldwork on a three-year study entitled 'Place, crime and insecurity in everyday life'.

Ian is also developing a new line of research on criminology and the harms of automobility. Ian has been awarded a Major Research Fellowship by the Leverhulme Trust to develop this work. The Fellowship begins in September and runs for three years. Ian is also teaching a new graduate seminar on 'Criminology and the car'.

Ian is Editor-in-Chief of the Howard Journal of Crime and Justice. Ian has recently been a member a member of the Advisory Board for the Strategic Review of Policing in England and Wales and of the Research Advisory Board of the Canada/Nova Scotia Mass Casualty Commission.

Ian supervises doctoral students working on the sociology of policing and security. He is particularly keen to work with students and post-doctoral researchers addressing problems of everyday in/securities, environmental harms, criminology and automobility, and the politics of security and justice.



Helen Millichap

Deputy Assistant Commissioner and Director, National Centre for VAWG & Public Protection

Helen joined the Metropolitan Police Service in 1997, starting in Newham, where she specialised in supporting

victims of sexual and domestic abuse. Through the years that followed, she worked in a range of both detective and uniformed leadership roles across many parts of London, including as the Borough Commander in the Royal Borough of Greenwich, and later, Haringey, and then as the first BCU Commander for the boroughs of Enfield and Haringey.

She has held the role of Commander for Learning and Development before becoming the Commander Protection, with responsibility for Royalty and Specialist Protection (RaSP) and Parliamentary and Diplomatic Protection (PaDP).

In 2023, Helen became the Deputy Assistant Commissioner for Local Policing and the Met's lead for tackling Violence against Women and Girls (VAWG). More recently, her responsibilities involved the portfolio of Trust and Legitimacy, including the delivery of culture reform. She continues to believe that success in each of these areas is critical to policing's role in protecting the public.

Helen was honoured to be awarded a Kings Policing Medal for Distinguished Service in overseeing protective security operations during the Platinum Jubilee celebrations, the funerals of the Prince Philip and Queen Elizabeth II, and the management of the Met's response to tackling VAWG.

In May 2025, she was appointed as the Director of the National Centre for Violence Against Women and Girls and Public Protection (NCVPP). Helen is proud to lead this collaboration between the National Police Chiefs' Council (NPCC) and the College of Policing, which is focused on supporting forces to achieve the highest possible standards for victims, bring more offenders to justice and continuing to tackle the ever-growing threat in this area by identifying and sharing innovative and effective practice.



Graeme Biggar

Director General, National Crime Agency

Graeme Biggar has led the National Crime Agency (NCA) since October 2021. The NCA is an intelligence-

led law enforcement agency whose

mission is to protect the public from serious and organised crime. It does that by leading the operational system response to ensure that police and law enforcement agencies are working together on the most significant threats, and by itself investigating and degrading the most harmful organised crime groups. The NCA also leads for UK policing on operational cooperation internationally.

Graeme initially joined the NCA in March 2019 as the Director General of the National Economic Crime Centre (NECC), which is a collaborative, multi-agency centre established to deliver a step change in the response to fraud and money laundering.

Prior to the NCA, Graeme was the Director of National Security in the Home Office, Chief of Staff to the Defence Secretary in the Ministry of Defence and held a range of other senior Civil Service roles.

Graeme has a degree in History from Oxford University and a masters in International Security Studies from the Royal College of Defence Studies and Kings College London. He was awarded a CBE in 2019 in recognition of his services to national security.



Paul Court

Deputy Chief Constable, Sussex Police and NPCC Lead for Violence Fixated Individuals

Paul is the Deputy Chief Constable of Sussex Police. Prior to this he worked for both Merseyside Police and the Metropolitan Police Service. Paul is also currently the national lead for the VFI (Violent Fascinated Individuals) portfolio and deputy lead for the national drugs portfolio'.



Dr. John Higham

Online Safety Policy Director, Ofcom

Jon Higham is Director of Policy Development in Online Safety Group at Ofcom, UK's communications regulator. He oversaw the development and delivery of Ofcom's recent consultation on protecting people from illegal harms online. Jon has worked on online safety since 2020 and has played a central role in developing Ofcom's approach to online regulation. Prior to working on online issues, Jon spent 12 years working in a variety of regulatory policy roles across Ofcom focusing on a range of sectors.



Alex Murray

Director of Police.AI

Alex Murray grew up around the world as an army child and graduated from Birmingham University in 1996. His partner is a sign language interpreter, and they have three children. Initially in West Midlands Police he worked in CID and uniform roles in the cities of Birmingham, Coventry and Wolverhampton.

He has been a senior investigating officer and has experience within Counter Terrorism. In 2008 he obtained a Masters from Cambridge University with a thesis that developed the understanding of police legitimacy within Muslim communities. He has been a specialist firearms, public order and CT commander. He was temporary ACC Crime in West Midlands for three years leading crime investigations, forensics, criminal justice and intelligence. He then became Commander, Specialist Crime in the Met leading teams specialising in cyber, human trafficking, child abuse and economic crime. In 2021/2022 he led on the policing of violence in London in response to heightened levels of teenage homicide. He has been the Chief Constable (Temp) of West Mercia Police delivering a people-led, tech-enabled, crime fighting vision of policing.

He recently has led the Serious Organised Crime Threats portfolio in the National Crime Agency. Currently he is seconded from the NCA into the position of temporary Director of PoliceAI – an organisation committed to delivering responsible AI in UK policing.

He is the founder of the Society of Evidence Based Policing and has worked on police training programmes in India, Cambodia and Europe. In 2017 he was awarded an OBE.



Chief Constable Jason Hogg

Thames Valley Police

Jason is the Chief Constable of Thames Valley Police and is responsible for all aspects of operational delivery covering the three counties of Berkshire, Buckinghamshire and Oxfordshire, which has a population of over 2.5 million. Nationally he is the National Police Chiefs' Council (NPCC) Chair of the Workforce Co-ordination Committee which includes Leadership, Wellbeing, Maintaining the Future Workforce, Professional Standards and Ethics, Pay and Review, Pensions and Inclusion of Culture. He is the NPCC lead for Drugs and the NPCC thematic lead for the Protect and Prepare strand of the Governments 'CONTEST', Counter Terrorism Strategy. He is also responsible, on behalf of the South East Region, for the delivery of Counter Terrorism Policing and the Organised Crime Unit. In addition, he is a member of the National Police Air Support Board, charged with delivering effective air services to Police Forces across the UK and the NPCC lead for Detective Resilience and Wellbeing.

Jason joined the police after studying for a BA (Hons) degree in Theology at Oxford University, and made the decision to apply to join the police after meeting two Thames Valley officers whilst working at a homeless centre as a student.

Jason started his career in Cleveland Police in 1995 and has also worked for Hampshire and the Isle of Wight Constabulary. He has spent most of his career working in Criminal Investigation roles, serving as a Detective in every rank. During his career he has been on extended secondments with Her Majesty's Inspectorate of Constabulary (HMIC) and the Foreign and Commonwealth Office (FCO) working overseas in Iraq.

Attendees

Alex Murray	Interim Director Police AI	Police AI
Alice Russell	Public Affairs Lead	Refuge
Andrew Fahey	Public Affairs Director	Forensic Analytics Ltd
Blair Gibbs	Director	The Police Foundation
Claire Bell	Deputy Director	National Centre for Violence Against Women and Girls and Public Protection
Claire Hammond	VAWG Delivery Lead	National Centre for Violence Against Women and Girls and Public Protection
Emma Feggetter	Managing Director - Police and Justice Lead	Accenture
Dylan Alldridge	Deputy Director	Strategy & Coordination, Police AI
Georgia Moore	Graduate Student	University of Oxford
Giles Herdale	Director	HDC Ltd
Graeme Biggar	Director General	National Crime Agency
Harry Leadbeater	UK Public Sector	Palantir
Helen King QPM	Principal, St Anne's College	University of Oxford
Helen Millichap KPM	Director	National Centre for Violence Against Women and Girls and Public Protection
Jason Hogg	Chief Constable	Thames Valley Police
Jason Pandya-Wood	Dean, School of Social Sciences	Western Sydney University
Joanne Walker	Research Specialist in Data and AI	BT Group plc
Jon Higham	Online Safety Policy Director	Ofcom - Office of Communications
Kate Algate	Strategic Director	VISAV Limited
Katie Hayman-Joyce	Policy and Public Affairs Manager	Molly Rose Foundation
Katrin Mueller-Johnson	Associate Professor of Criminology	University of Oxford
Larry Sherman	Chair	Cambridge Centre for Evidence-Based Policing
Maeve Walsh	Director	Online Safety Act Network
Maggie Blyth KPM	Chief Constable	Gloucestershire Constabulary
Martin Tunstall	Chief of Staff	NPCC
Neil Basu QPM	Senior Fellow	The Police Foundation
Nouf Al Anezi	Policy & Campaigns Officer	Suzy Lamplugh Trust
Paul Court	Deputy Chief Constable	Sussex Police

Attendees

Professor Ian Loader	Professor	All Souls College, University of Oxford
Rebecca Hitchen	Head of Policy and Campaigns	End Violence Against Women Coalition (EVAW)
Rich Muir	Policing Advisor to the Home Secretary	Home Office
Sara Thornton DL QPM	Chair of Trustees	The Police Foundation
Sian Penny	Public Safety & Justice Director	BT
Sumaiya Zahoor	Policy Manager	Internet Watch Foundation
Zoe Manzi	Senior Analyst, Hate and Extremism	ISD

© 2026: The Police Foundation

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, without the prior permission of The Police Foundation.

Enquiries concerning reproduction should be sent to The Police Foundation.

Email: info@police-foundation.org.uk

www.police-foundation.org.uk

Charity Registration Number: 278257

THE
POLICE
FOUNDATION

The UK's policing think tank