Association of Police and Crime Commissioners

APCC REPORT: Response of Police and Crime Commissioners to online safety

Last update: 03/04/2025

This report examines the current response to online safety and online harms by Police and Crime Commissioners (PCCs) with recommendations for next steps.

TABLE OF CONTENTS

Introduction

Online safety is a growing problem with increasing reports and high-level media coverage, and with strong links to violence against women and girls (VAWG), fraud and cybercrime. With the passing of the Online Safety Act 2023 and growing concerns across policing, the Association of Police and Crime Commissioners (APCC) undertook an exercise to review the response to online safety from Police and Crime Commissioners, Police, Fire and Crime Commissioners, Deputy Mayors for Policing and Crime and Chairs of Relevant Authorities (hereafter referred to as 'PCCs').

This report aims to support PCCs in reflecting on their local practice through the sharing of an analysis of current activity and notable practice and by providing recommendations for future work.

What is online safety?

The Online Safety Act 2023 (OSA)[1] defines online safety as the protection of children and adults from harmful content and behaviour online.

The regulator of the OSA is Ofcom,[2] who are responsible for enacting regulatory provisions within the Act by March 2025. New offences introduced by the OSA took effect in January 2024.[3]

Harmful content and behaviour fall under two strands:

- Online harms
- Online offending

Online harms

The OSA defines online harms as:

- User-generated content or behaviour that is illegal or could cause significant physical or psychological harm to a person
- Harmful information that is posted online or sent to a person
- Content that is illegal and harmful that online platforms must monitor and remove

Not all online harms are illegal, but they can still have devastating impacts on victims who need support.

[1] Online Safety Act Explainer – Published 8 May 2024: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer
[2] Ofcom: Online Safety: https://www.ofcom.org.uk/online-safety/
[3] Online Safety Act – new criminal offences circular: https://www.gov.uk/government/publications/online-safety-act-new-criminal-offences-circular/online-safety-act-new-criminal-offences-circular

Examples of online harms include:

Illegal

- Child sexual abuse and exploitation (CSA/CSE) material
- Content promoting terrorism
- Fraud
- Intimate image abuse

Not illegal

- Content promoting eating disorders or destructive behaviours
- Online harassment that does not meet the definition of an offence
- Catfishing

Online offending

Online harms that are illegal in the OSA will also meet the definition of Online Offending. Further online offences are listed within the Computer Misuse Act (CMA) 1990.[4]

Examples of CMA offences include:

- Unauthorised access, entering a computer system without permission, also known as hacking
- Unauthorised access with intent to commit a further offence, using a computer system to steal data, destroy a device, or plant a virus
- Unauthorised modification of data, such as modifying or deleting data, or introducing malware such as viruses, adware, or spyware
- Unauthorised acts with intent to impair computer operation
- Unauthorised acts causing serious damage, like hacking into a police network and causing delays to emergency calls
- Making, supplying, or obtaining articles for use in computer misuse offences, such as downloading software to bypass login credentials

[4] Computer Misuse Act 1990: https://www.legislation.gov.uk/ukpga/1990/18/contents

Summary of recommendations

Recommendation 1: Language and terminology around online harms should be consistently applied to increase public awareness and confidence in reporting.

Recommendation 2: Where PCCs are undertaking activity to raise awareness of the risk of online harms there should be opportunities to share practice and approaches.

Recommendation 3: Data and evidence collection on the prevalence and impact of online harms should be improved.

Recommendation 4: The public should be encouraged to report online crime when it happens. PCCs and forces should ensure that they are working to increase awareness amongst the public and staff, and that policing can respond effectively to reports of online offences.

Recommendation 5: PCCs should have tools and guidance to support them in holding chief constables to account for force performance on online harms and chief constables should be supported to share appropriate evidence.

Recommendation 6: The implications of the Online Safety Act on policing and local policing governance should be made clear for PCCs and partners.

Recommendation 7: Respecting local structures, PCCs and forces should ensure online harms are included within wider strategic and operational governance structures including forums related to violence against women and girls.

Recommendation 8: PCCs should consider how best to engage victims of online harms to further understand what support they need, and how many are accessing services.

Recommendation 9: Where there are examples of services that can support victims of online harms these should be identified and shared. Providers should be engaged to share practice and supported to keep pace with the fast-changing demand presented by online harm offences.

Background

The APCC's engagement with the online safety agenda has included:

- Engaging with parliamentarians to influence the Online Safety Act
- Responding to Ofcom's consultations into online safety regulations
- Distributing resources to PCCs such as a briefing on the metaverse

The APCC undertook a review into online safety to build our understanding of how PCCs are engaged on this issue, identify notable practice and consider what further support we might provide.

Methodology

We undertook a scoping exercise, engaging with national and local stakeholders, to develop an evidence base and identify key themes to explore via targeted engagement with PCCs.

Those stakeholders included:

- City of London Police and its Authority
- National Police Chiefs Council (NPCC) VAWG Taskforce
- NPCC National Cyber Portfolio
- Ofcom
- Home Office
- Department for Science, Innovation and Technology (DSIT)
- Local forces
- Commissioned victim services such as Victim Support and The Cyber Helpline
- Police and Crime Commissioners, and Offices of PCCs (OPCCs)
- University College London (UCL)
- Worshipful Company of Information Technologists (WCIT)

The APCC subsequently developed and distributed a survey to PCCs, focusing on three thematic areas:

- Awareness of online harms
- Performance
- Victims' services

We received responses from **18 PCCs** (listed in Annex A) from across England and Wales and had supplementary conversations with a further four PCC offices to provide more in depth evidence.

Findings

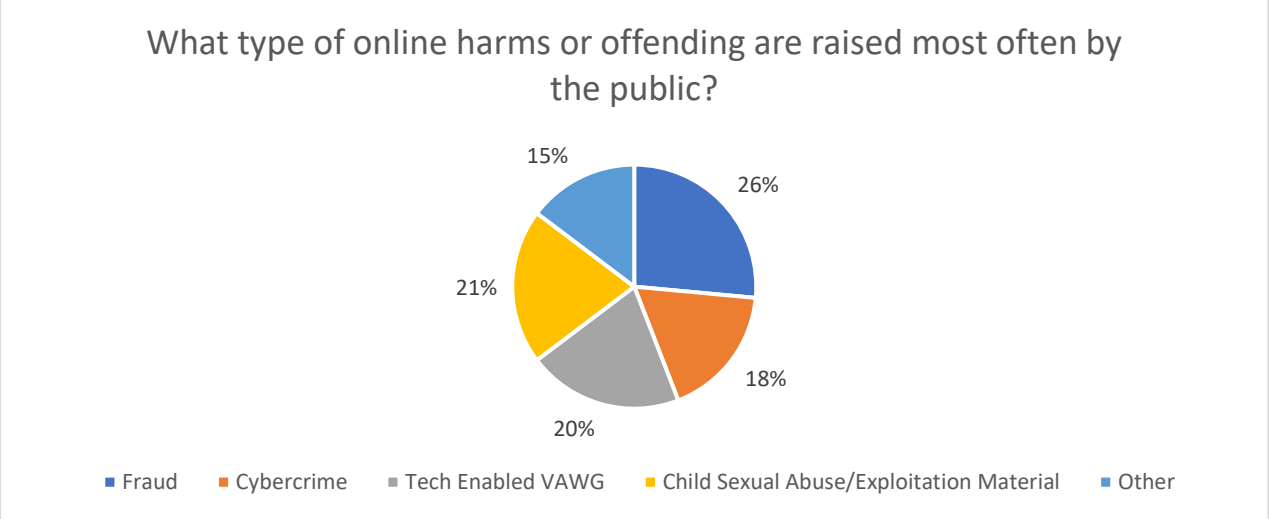
The following is a thematic analysis of the findings of the survey and the wider engagement with PCCs and OPCCs.

Awareness of online harms

PCCs have an important role in raising awareness of harmful issues and behaviours and undertaking preventative activity. Through engagement with their local communities PCCs reported that the public are raising concerns about online harms and offending.

Table 1 provides a breakdown of online offences raised, where PCCs were able to select multiple categories:

Table 1



Fraud and cybercrime, which are closely interconnected, account for 44% of offending raised most often by the public. This is then followed by tech enabled VAWG and child sexual abuse/exploitation material.. Of the five PCCs who selected 'other', four reported fraud as the most raised concern and emphasised the underreporting of this crime type amongst the public.

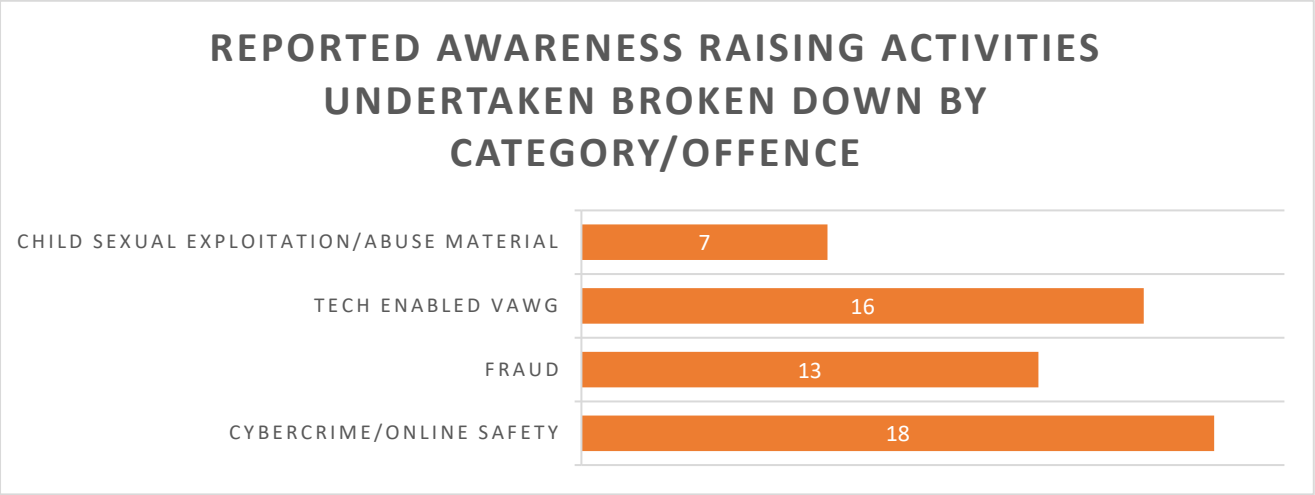
PCCs are engaging their communities to raise awareness of offences and remind the public of the dangers of online spaces. PCCs highlighted a number of initiatives:

- Award schemes
- Awareness days, communications and media campaigns
- Funding educational books and materials
- Hosting summit and/or roundtables with agencies and partners

- Collaborative activity with partners such as local authorities or education

PCCs focused awareness raising activity across several critical areas broken down in Table 2.

Table 2



Despite being the least common offence raised during engagement with communities, cybercrime/online safety was the most common issue in awareness raising activities reported by the PCC. It may be that cybercrime is conflated with other offences such as fraud and tech enabled VAWG, which could explain the disparity between awareness raising activities and offences raised during community engagement.

Recommendation 1: Language and terminology around online harms should be consistently applied to increase public awareness and confidence in reporting. The APCC will develop a factsheet and supporting documents to support PCCs in understanding and communicating the threat and risk of online harm to partners and the public.

Durham PCC – Commissioner's Challenge Platinum Award Schemes

In early 2024, Durham PCC designed the Commissioner's Challenge Platinum Award Schemes for the theme of cyber safety in the area. This is an interactive safety project that had previously engaged thousands of young people across County Durham and Darlington and has now been rolled out to a secondary school to keep older children safe. For one award scheme, around 180 students at a local school were offered the chance to undertake a cyber challenge, all those who successfully completed the modules were entered into a prize draw with the opportunity to win an iPad. The activities focused on how pupils and their families can stay safe online with the overarching aim to equip young people with the knowledge they need to make safe choices now and in the future. Since the programme was rolled out county-wide, more than 3,000 primary school pupils have signed up.

Hampshire and the Isle of Wight PCC – Cyber Ambassador Scheme

The Hampshire and Isle of Wight PCC previously established the Cyber Ambassador scheme. Under the Cyber Ambassador Scheme, groups of students received training at school and shared this knowledge and offered support to their peers.

The scheme aims to keep young people and families safe online, with ongoing engagement, updates, and advice on issues such as scams, gaming, and online safety. While the OPCC continues to deliver the 'train the trainer' model, the scheme's resources have now been adopted nationally by the National Cyber Security Centre.

PCCs considered the need to raise awareness of victims' rights and increase public knowledge of online harms and offending. General understanding of the new offences introduced within the Online Safety Act may still be limited and many victims do not know that they are experiencing crimes. This further contributes to the significant underreporting in this area.

Additionally, PCCs raised concerns around the education gap around tech-enabled VAWG and wider online harms in schools and youth spaces, and the need for preventative activity. For example, incidents are emerging of young people, and typically boys, using widely accessible 'nudity'/undressing apps to create and distribute AI-generated images of their peers (typically girls).

Recommendation 2: Where PCCs are undertaking activity to raise awareness of the risk of online harms there should be opportunities to share practice and approaches. The APCC will facilitate opportunities to share notable practice and identify collaborative approaches with partners to implement learning.

The impact of online harms

Online harms and offences can have a devastating impact, both visible and invisible, on communities. With the offences perpetrated online in a highly personal and private but equally public environment, there are countless opportunities for criminals to exploit victims. There is a clear impact on individuals' online confidence. In an increasingly online society, a lack of confidence in using online services for an extended period can have a serious impact on the individual and the delivery/access of public services.

PCCs reported using several qualitative and quantitative sources to measure the impact of online harms and offending:

- Feedback and data from commissioned victims' services
- Community engagement
- Case studies
- Crime statistics from a national service
- Operational force data

The majority of PCCs reported that they predominantly use operational force data and victims' services data to measure impact. Operational datasets may use 'flags' within the data to highlight offences where online offending has been a factor. However, data drawn from victims' services may be more individualised and consider the impact of the offence, for this reason it will also tend to be more qualitative and contain sensitive information. When used together, these data sets are complementary and provide a richer picture of the issue.

PCCs and forces utilise quantitative data such as operational data to measure reporting, including:

- National Crime Survey
- Office for National Statistics - Crime in England and Wales
- HMICFRS Digital Crime and Performance Pack
- National Data Quality Improvement Service

South Wales PCC – National Data Quality Improvement Service

The South Wales PCC drew on national data bases such as the National Data Quality Improvement Service (NDQIS) for 'online crime', run by the Home Office. This allows the force to capture an increased pool of data to measure the impact of online harms and offending in their communities. In doing so identifying offences as online that are not identified as such in the first instance.

PCCs noted the difficulty in concretely measuring the impact of this type of offending and the associated harms. Qualitative evidence is important in evidencing the impact and was obtained through engagement with the public directly and by collating case studies. They may also take feedback from commissioned services and utilise data collection from those services to understand the prevalence and impact of offending.

The NPCC have identified that 7% of police recorded VAWG offences could be identified as 'online' but that 'police recorded crime data is almost certainly underrepresented'.[5] The underreporting of VAWG offences is due to a complex mix of reasons, including a lack of public understanding of what constitutes an offence, a lack of trust in policing response to VAWG, and feelings of shame. PCCs also highlighted the issue of underreporting, noting that there is a lack of understanding of what is and is not a criminal offence, meaning that, in some cases, victims do not know that they are experiencing crimes. This compounds the significant underreporting of online harms and detrimentally affects our understanding of the impact on victims.

Online offences and harms can translate into the physical world. PCCs said that their forces were recognising that online offences can transition into physical criminality, especially in cases involving domestic abuse, stalking, or sexual violence. The NPCC Policing Statement for Violence Against Women and Girls (2024) highlighted that of the 123,515 VAWG offences with an online element in August 2022- July 2023, 39% were related to domestic abuse flags and that stalking and harassment accounted for 85% of all online and tech-enabled VAWG. Others have recognised a link between social media and youth violence. Individual cases have been highlighted by victims' services, including Independent Sexual Violence Advisers (ISVAs) and Independent Domestic Violence Advisors (IDVAs), providing further examples of such instances.

However, the majority of PCCs were not tracking cases that started offline and then went online and vice versa. PCCs noted the need for further research in this area to better understand the

[5] National Policing Statement 2024 For Violence Against Women and Girls (VAWG) https://news.npcc.police.uk/resources/vteb9-ec4cx-7xgru-wufru-5vvo6

translation from online offending and harms to offline harm and to improve data and evidence collection linking offences.

Recommendation 3: Data and evidence collection on the prevalence and impact of online harms should be improved to support understanding.

The APCC will coordinate practice sharing through our Economic and Cyber Crime and Performance portfolios.

We will work with partners in the NPCC and Home Office to consider ways to better flag cases involving online offences.

We will work with partners in the Centre for VAWG and Public Protection to understand how better to understand the interaction between online and offline offending in relation to VAWG offences.

According to the Crime Survey for England and Wales (CSEW) for the year ending March 2024,[6] fewer than 1 in 14 computer misuse offences were reported to the police or Action Fraud. In the CSEW year ending September 2024, there were approximately 867,000 computer misuse offences.[7] In a recent 2025 Home Office publication, it was noted that there are several enablers and barriers to reporting.[8] For crime types like fraud and cybercrime, Action Fraud is the national reporting centre. The Home Office report shows a lack of awareness among victims taking part in the research that this organisation existed. Instead, victims reported to organisations that they believed would be most able to resolve the situation. This should include their bank/building society, social media platform or the online selling platform where the cybercrime or fraud had taken place. However, some reported the crime directly to the police or Action Fraud.

[6] Crime Survey for England and Wales – Office for National Statistics – year ending June 2024: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2024#computer-misuse

[7] Crime in England and Wales: year ending September 2024 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2024#computer-misuse

[8] Understanding the cybercrime and victim journey – Home Office – year ending January 2025 https://www.gov.uk/government/publications/understanding-the-cyber-crime-and-fraud-victim-journey/understanding-the-cyber-crime-and-fraud-victim-journey#reporting

PCCs also recognised the need to provide appropriate support to victims and survivors and ensure effective engagement in assessing how best to deliver that support and to properly understand the impact of such crimes.

Recommendation 4: The public should be encouraged to report crime when it happens. PCCs and forces should ensure that they are working to increase awareness amongst the public and staff, and that policing can respond effectively to reports of online offences

The APCC will facilitate and share the sharing of PCC and partner approaches to raising awareness (Recommendation 2).

PCCs and chief constables should ensure that staff receive appropriate training to manage reports, and the College of Policing should ensure training is available.

Performance and accountability

Online safety may form part of a PCC's police and crime plan and is one of the five critical threats identified in the NPCC's VAWG Statement 2024[9]. In addition, HMICFRS' assessment of police effectiveness, efficiency and legitimacy (PEEL) includes renewed focus on the force's local response to managing fraud, including online fraud. The PEEL process exists to promote improvements in key aspects of policing by identifying where forces need to improve and to help the public understand how well their force is performing.

PCCs must also have regard to the Strategic Policing Requirement (SPR) when issuing or amending their Police and Crime Plans, and provide an assurance statement within Annual Reports, explaining how they have had regard to the SPR. Under the SPR, Serious and Organised Crime (SOC) is identified as a key threat, with cybercrime and fraud highlighted as categories of SOC.

Responding to the APCC survey, PCCs reported several mechanisms through which they hold their CC to account on online harms and offending:

- Scrutiny/performance meetings
- 1 to 1 meetings between the PCC and CC

Quantitative data is used to support these conversations. PCCs reported utilising the following performance measures:

- Victim satisfaction surveys and feedback

[9] National Policing Statement 2024 For Violence Against Women and Girls (VAWG) https://news.npcc.police.uk/resources/vteb9-ec4cx-7xgru-wufru-5vvo6

- His Majesty's Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS) Digital Crime and Performance Pack
- Office for National Statistics (ONS) crime survey data
- Force crime data
- Force performance reports
- Case studies

Many PCCs noted the need for further support in holding chief constables to account. Further guidance on the following might be beneficial:

- Definition of online harms
- How to measure police performance and direction to data sources
- How the Online Safety Act will affect demand and expectation on operational partners.

Recommendation 5: PCCs should have tools and guidance to support them in holding chief constables to account for performance on online harms and chief constables should be supported to share appropriate evidence. The APCC will develop a '10 questions for your Chief Constable: Online Safety' to enhance scrutiny and accountability, working with policing partners. This will form part of the wider '10 Questions' 'series.

Recommendation 6: The implications of the Online Safety Act on policing and local policing governance should be made clear for PCCs and partners. The APCC will work with the Department for Science, Innovation and Technology (DSIT) and partners to provide guidance to PCCs.

Governance

While PCCs primarily hold chief constables to account through the mechanisms outlined in the previous section, they engage in additional governance structures or forums which include monitoring of the response and activity on online harms and offending.

No PCC reported having a dedicated governance structure for online harms and offending, however it may fall into existing VAWG governance structures, such as VAWG or DA Boards, Community Safety Partnership Boards, force-led VAWG Gold Groups, and Independent VAWG Scrutiny Panels. Equally, the issue may be addressed through community scrutiny boards or victim programme

boards. This may allow online harms to be addressed holistically amongst wider issues in the VAWG space rather than addressed in isolation.

While not raised in responses to the survey, online offending should also form a part of multi-agency risk assessment forums, such as multi-agency risk assessment conference (MARAC), Multi-agency tasking and coordination (MATAC) and Multi-agency public protection arrangements (MAPPA).

Recommendation 7: Respecting local structures, PCCs and forces should ensure online harms are included within wider strategic and operational governance structures, including forums related to violence against women and girls.

Victims' support services

PCCs have a crucial role in commissioning services to support victims and survivors of crime including for those affected by online offences. While PCCs are aware of the rise in online harms as a crime type, and the impact on victims, the majority of PCCs surveyed reported that they did not commission a specialist service for victims of online offences.

Victims of online offences may be offered support through:

- Commissioned multi-crime services or Victims' Hub
- Independent Sexual Violence Advisors (ISVAs)
- Independent Domestic Violence Advisors (IDVAs)
- National Economic Crime Victim Care Unit (NECVCU)
- Charitable organisations
- Fraud caseworkers/hubs
- Stalking services

While there was confidence among some PCCs in the adequacy of these services for supporting victims of online offences, other PCCs noted the difficulty in measuring the effectiveness of this support. Due to the changing nature and increasing pace of cyber offending, services are catching up to ensure that victims are identified and provided with the right support. Research is required to better understand the issue and develop the right support and preventative activity.

PCCs noted the uncertainty around future funding post 2025/26 for victims' core services and in ensuring there is a sufficient resource to deal with large numbers of victims of online crime, creates further challenges to providing support.

While victims may be referred to support after contacting the police, they are also able to self-refer to PCC commissioned services. PCCs surveyed did not measure referral rates to commissioned

services of victims of online offences. Often these offences may be secondary to a primary offence, such as stalking, so victims will be referred for support for the higher tariff offence. Additionally, as the data is not routinely collected, or a requirement for the MoJ for grant return, PCCs would need to undertake a resource intensive deep dive.

Without a clear picture of the number of victims accessing support for offences committed online, PCCs will find it difficult to target funding as effectively. The online landscape is changing at pace, and commissioned services may struggle to react to emerging crimes and effectively support victims of those crimes. It is important that the right support is identified, and this is more challenging where victims may have multiple needs and may have experienced multiple forms of criminality.

Recommendation 8: PCCs should consider how best to engage victims of online harms to further understand what support they need, and how many are accessing services.

The APCC will engage with services nationally to encourage evidence gathering.

The Ministry of Justice might consider how it collects annual data returns in relation to online safety.

The majority of PCCs highlighted the need for consistent training and education for victim service providers to better understand emerging harm, new technologies and systems. They noted the need for cybercrime specialists to communicate changes in the methods of online offending to service providers. They identified the lack of industry wide training to up-skill service providers, particularly around fraud and sexual offences, to ensure they can support victims most effectively and signpost to specialist support.

Durham PCC: Feedback from ISVA Service Provider

When Durham PCC gathered information from service providers for the rape and sexual abuse service, they recognised a knowledge gap across the staff and volunteer team on online harms.

Victim services in Durham have said:

ISVA service provider

I had a client whose intimate pictures were published online by her ex-boyfriend. She reported it to the police, they seized his devices, but unfortunately he took his own life so the investigation was closed. The client struggled with removing the pictures from online services, and she kept finding new websites. I believe the images are still online. The Police said that they couldn't do anything about it. Changing Lives were helping with this, but I think they couldn't do much. I signposted her to the Revenge Porn helpline or similar website, but If I remember well they couldn't help because some of the pictures were taken when she was underage.

In this situation, the level of harm to the victim was compounded by the complexities of the crime type. Not only was there an element of revenge porn, but intimate image abuse and any rippling effect of hearing about the death of a previous partner. Likewise, there is a lack of trust in the police and in the system as the victim struggled to get a clear response and outcome to her situation. The ISVA acknowledged that they were not equipped to respond to complex situations like this and further knowledge of helplines and specialist provisions are needed.

Recommendation 9: Where there are examples of services that can support victims of online harms these should be identified and shared. Providers should be engaged to share practice and supported to keep pace with the fast-changing demand presented by online harm offences. The APCC will work with providers and engage government colleagues and other partners such as academics, Ofcom, and cyber-specialised services to identify notable practice and support in sign-posting to up-skilling opportunities for PCCs and services.

Conclusions

This report has demonstrated a clear need for further exploration on the fast-rising issue of online safety across several high priority areas. There is a significant and very real risk to the public across offences from tech-enabled VAWG, to child sexual exploitation and fraud. All have very damaging and long lasting impacts on victims and survivors, and the concerning link between online and offline offences cannot be overstated.

The recommendations represent small steps that may be taken in developing the response from PCCs in working with our partners, and in improving our response to online harms. The nine recommendations address the findings in the report.

While PCCs recognise the threat raised by online harms, there is a lack of clarity regarding role and expectations and a need to provide guidance to support PCCs and partners in driving performance locally.

Where there is good practice, we must identify and create opportunities to share widely across our partners. We must also bring in those with the expertise to develop and build new approaches to provide the best advice and guidance.

We must be collaborative in working with our partners to build our understanding of the risk and threat associated with online harms, developing better data and evidence and driving forward innovative approaches to pursuit and prevention.

PCCs are also heavily engaged in raising awareness of critical issues and ensuring online harms do not go unreported. It is important that the public is made aware of the risks.

Next steps

The recommendations arising from this report will be actioned through the APCC into 2025/26.

We will engage partners on the recommendations to ensure an aligned approach and work with them on their priorities in the online harms and safety space. This will include working with the new Centre for VAWG and Public Protection, the NPCC National Cyber Programme, City of London Police, Ministry of Justice and others.

Annex A: List of respondents

The following is the list of PCCs who responded to the survey and contributed to the findings of this report:

- Derbyshire
- Durham
- Essex
- Gloucestershire
- Hampshire and Isle of Wight
- Hertfordshire
- Greater Manchester Combined Authority
- Merseyside
- Mayor of London's Mayors Office for Policing and Crime
- North Wales
- North Yorkshire Combined Authority
- Northumbria
- South Wales
- Surrey
- Thames Valley
- Warwickshire
- West Midlands
- West Yorkshire Combined Authority

Contact us

Association of Police and Crime Commissioners
Lower Ground, 5-8 The Sanctuary, Westminster, London SW1P 3JS

Telephone: 020 7222 4296
Website: www.apccs.police.uk
Email: apccsgeneral@apccs.police.uk

The APCC provides support to all Police and Crime Commissioners and policing governance bodies in England and Wales.

Document authors:

Joe Dunbar, Policy Assistant

Kavisha Rodrigo, Policy Officer

Ella Thomas, Senior Policy Officer

Association of Police and Crime Commissioners