TRAINING NEEDS ANALYSIS

The Police Response to *Technology-Facilitated Abuse*

A practitioner-focused assessment of current knowledge, skills, gaps and training priorities across policing and partner agencies in England and Wales

Authors: Giles Herdale, Dr Keely Duddin, Dr Hannah Guy and Professor Olga Jurasz

September 2026

Centre for Protecting Women Online | The Open University | protecting-women-online@open.ac.uk

Foreword

This Training Needs Analysis (TNA) is published at a time of growing recognition, in policy, in research, and among victim and survivor advocates, that the police response to technology-facilitated abuse remains deeply inconsistent and, for many victims, inadequate. That is not a comfortable finding, but it is a well-evidenced one.

Research has consistently documented the ways in which institutional cultures within policing can minimise victims' experiences, reproduce disbelief and secondary victimisation, and undermine confidence in police responses to violence against women and girls (Hohl & Stanko, 2022). Emerging research, alongside national policing and government strategies, suggests that these challenges extend to technology-facilitated abuse, where digital harms may be underestimated and responses remain inconsistent (Douglas et al., 2025; National Police Chiefs' Council, 2024; Home Office, 2025).

At the same time, the picture is not uniform. This TNA has drawn on contributions from officers and staff across more than twenty forces who are working hard, often without dedicated resource or national support, to build meaningful responses to technology-facilitated abuse. The expertise that exists within policing on this issue is real and, in places, impressive. The problem is that it is unevenly distributed, insufficiently resourced, and not yet embedded in the kind of national training and operational infrastructure that would make it the norm rather than the exception.

The Centre for Protecting Women Online is a University-based research centre at The Open University. Our work is grounded in the evidence base, in partnership with victims and survivors, and in ongoing collaboration with policing and partner agencies. This TNA has been produced in that spirit. It names problems honestly, because honest evidence is what enables change. The recommendations that follow are directed primarily at national policing bodies, the College of Policing, and government, because sustainable improvement requires national leadership, not just individual commitment at force level.

We hope this report is useful to those within policing and other organisations who are already making the case for better, and that it provides the evidence base to support them in doing so.

Dr Keely Duddin. Policing Stream Lead, Centre for Protecting Women Online

The Open University, September 2026

Executive Summary

This Training Needs Analysis (TNA) was commissioned to inform the operational development of the police response to technology-facilitated abuse (tech abuse). It is a practitioner-focused exercise designed to surface current practice, skills gaps and training requirements across policing in England and Wales and partner agencies across the UK. It is not a research study and does not seek to generate generalisable academic findings; rather, it draws on the experience and expertise of policing professionals and sector stakeholders to inform operational decision-making.

The threat of tech abuse has grown significantly in recent years. The government's Violence Against Women and Girls (VAWG) strategy (2025) recognises that VAWG offences *"are increasingly perpetrated online, with new and evolving forms of digital abuse driving an ever-growing impact on young people."* Referrals to Refuge's specialist tech abuse service rose by 62% in 2025 (Refuge, 2026), and the Domestic Abuse Commissioner has warned that devices and social media are being "weaponised by abusers to control" survivors at scale.

Despite this growing recognition, a significant gap persists between the scale of the problem and the practical policing response. This gap has undermined both victim trust and confidence in policing, and has hampered delivery of the government's ambitions on VAWG.

This TNA draws on a desk review of existing learning products and guidance, structured conversations with expert stakeholders, and a sector-wide call for input from policing organisations and frontline staff. Input was received from approximately 40 contributors across more than 20 forces and policing organisations. It identifies five key findings and a set of targeted recommendations.

This TNA was conducted to capture:

- Existing provision of knowledge and skills across policing
- Requirements for addressing identified gaps in knowledge and capability
- Lessons from local and regional initiatives
- A framework for a proposed national knowledge and skills programme

Key Findings

Finding 1

Awareness is growing, but from a low base

Forces generally recognise tech abuse as a strategic threat. However, awareness tends to start from a low knowledge base. Tech abuse is frequently characterised as an 'emerging' rather than core element of VAWG response, and is not routinely integrated into mainstream policing approaches such as domestic abuse investigation.

Finding 2

There is no national training framework

There is no current national police training or guidance on recognising or responding to tech abuse, and no agreed definition of what 'good' looks like. The College of Policing Op Modify e-learning package is patchy in uptake and not integrated into national VAWG training programmes such as DA Matters. Awareness of Op Modify is uneven, with many frontline officers reporting they are unaware of it.

Finding 3

Local initiatives exist but are uncoordinated

A number of forces have developed local or regional tech abuse training initiatives driven by dedicated professionals. Some are ambitious in scope. However, these initiatives are uncoordinated, often time-limited, and dependent on the personal commitment of a small group of motivated individuals rather than an embedded system-wide response.

Finding 4

The pace of change is outstripping capability

There is widespread recognition that tech abuse is a fast-moving and growing threat. Emerging harms such as generative AI misuse, deepfake imagery, voice cloning, spyware apps and wearable surveillance devices are identified as significant concerns for which training has not yet kept pace. Horizon scanning capability across forces is limited.

Finding 5

A national, coordinated response is essential

The evidence points to a clear and urgent need for a nationally coordinated approach encompassing NCVPP leadership, a comprehensive National Operating Model covering identification, response and partnership working, and sustained mainstreaming of tech abuse into core VAWG and public protection training, informed by the principles and experience of Operation Soteria.

Recommendations

1. The National Centre for VAWG and Public Protection (NCVPP) should proactively identify, map and co-ordinate existing local and regional tech abuse training initiatives, and develop a mechanism for scaling successful models nationally, drawing on the regional delivery infrastructure already demonstrated by cyber protect networks.

2. The College of Policing, supported by NCVPP, should integrate tech abuse as a core component of DA Matters, the mandatory frontline domestic abuse training programme. There is currently no specific tech abuse content within this programme and this gap should be addressed as an immediate priority within the current DA Matters review cycle.

3. The Home Office and NCVPP, building on the principles and infrastructure of Operation Soteria, should develop a National Operating Model for domestic abuse that integrates tech abuse as a core strand, encompassing identification, evidence preservation, digital safeguarding and specialist referral pathways.

4. The NCVPP, working with the College of Policing and specialist third sector organisations with expertise in tech abuse, should establish a national community of practice to share emerging good practice, develop investigative guidance, and ensure that learning from operational casework is systematically fed back into training and policy development.

5. The Home Office, NCVPP and College of Policing should jointly establish a multi-disciplinary horizon scanning function for technology-facilitated VAWG, linked to the national police.ai programme, to ensure that emerging threats including generative AI misuse, deepfake abuse, stalkerware and wearable surveillance technologies are tracked systematically and reflected in training content on a rolling basis.

6. HMICFRS should ensure that force responses to technology-facilitated abuse are included within the PEEL* assessment framework as a discrete strand, providing national accountability, consistent benchmarking and a lever for improvement across all 43 and relevant specialist forces.

*PEEL (Police Effectiveness, Efficiency and Legitimacy) is HMICFRS's programme for assessing how well police forces in England and Wales are performing, including how effectively they prevent and investigate crime, manage resources, protect vulnerable people and provide a legitimate and fair service to the public.

Introduction

The police response to technology-facilitated and online VAWG is a recognised and growing national policing priority. The VAWG strategy published in December 2025 acknowledged, for the first time, the centrality of tech abuse and harassment within the overall VAWG threat. It committed to:

> ***"Equip police officers and staff with the capability and evidence-based guidance they need to respond effectively to violence against women and girls."***
> ***- VAWG Strategy, 2025***

The strategy further committed that through the NCVPP, the learning from Operation Soteria would be used to ensure academic expertise informs new VAWG training and guidance for policing.

The current police response to tech abuse was the subject of a landscape review published by the Centre for Protecting Women Online (CPWO) in 2025 (Herdale, Duddin and Jurasz, 2025). The landscape review identified a range of challenges hindering the policing response, including under-recording and inaccurate recording practices; poor initial responses when victims come forward; missed opportunities to identify and preserve digital evidence; and an inability to recognise and link patterns of abuse beyond individual incidents. The review identified promising practice locally but found that these initiatives were scattered and inconsistently applied, with no national operating model to guide or track the police response

Why was this TNA commissioned?

This TNA was commissioned on the basis that:

- Tech abuse is a growing problem affecting an increasing number of victims and survivors
- There has been a lack of national focus on policing responses to tech abuse, and many frontline officers lack the skills and knowledge to identify and respond to it
- This lack of focus has adversely affected reporting of tech abuse and undermined confidence in the wider police response to VAWG
- There has been a growing recognition of the need for, and the role of, a policing response to TFVAWG in international policy instruments (e.g. Council of Europe Recommendation of the Committee of Ministers to member States on accountability for technology-facilitated violence against women and girls, 2026).

The findings of the previous landscape review (Herdale, Duddin & Jurasz, 2025) informed the need for this TNA, alongside developments over the subsequent twelve plus months since its publication. In this period, the salience of tech abuse has grown considerably, but without a commensurate focus on mitigation, particularly at the national level.

What is the challenge?

As technology has become embedded in everyday life, its impact on crime and criminal investigation has become increasingly clear. Smartphones, ubiquitous connectivity and the rapid development of artificial intelligence (AI) have accelerated this shift significantly. Approximately half of crime now takes place online (National Crime Agency, 2026), itself almost certainly an underestimate. Policing has responded through iterative developments, including specialist cyber-crime units dating back to the early 2000s. However, as technology has become embedded across virtually every crime type, reliance on specialist capability alone is no longer sufficient. Technology should therefore no longer be viewed as a specialist policing issue, but as a core operational capability required across the policing workforce.

VAWG is a national policing priority, but there has been longstanding inconsistency in specialist capability and resources across forces relative to other threat areas such as counter-terrorism and serious and organised crime. Referrals to public protection teams across policing rose by 37% without any commensurate increase in resources (NPCC & College of Policing, 2024). The workforce and deployment model for VAWG investigations creates additional challenges: Domestic abuse-related crime accounted for 15% of all police-recorded offences in England and Wales in the year ending March 2025 (ONS, 2025), yet Operation Soteria research has found that many RASSO investigators are more junior and less experienced than their counterparts in other high-risk policing areas (Hohl & Stanko, 2022), and face very high levels of stress, burnout and trauma (Sondhi et al., 2023; 2025).

The challenge of improving skills and knowledge to address tech abuse therefore operates at multiple levels, from raising awareness among frontline and response officers to ensuring that digital investigation specialists such as Digital Media Investigators (DMIs) can respond effectively to fast-moving technological developments.

Methodology

This TNA was conducted as a time-limited consultancy exercise drawing on multiple sources of input from across policing and partner organisations:

- A desk review of existing learning products, guidance and publicly available resources
- Structured conversations with a range of expert stakeholders, including senior police officers and third sector specialists
- A structured call for input on existing tech abuse training provision, circulated to police forces
- Attendance at a session of the College of Policing Digital Investigation Advisory Group (DIAG) and the NCVPP conference

As a time-limited exercise, this TNA does not claim to represent the views of every force. Input was received from approximately 40 contributors across more than 20 forces (in England & Wales) and other policing organisations across the UK, including national policing bodies, regional organised crime units, and a mix of urban, rural, county and metropolitan forces. Expert engagement included:

- College of Policing and NCVPP, including attendance at the Digital Investigation Advisory Group in January 2026
- Industry experts, including members of the TechUK VAWG and RASSO working group
- Policing experts, including senior leaders, public protection and digital investigation specialists
- Third sector experts, including training leads from Refuge and SafeLives

Contributors span roles from strategic public protection leads to frontline officers, Digital Media Investigators and cyber specialists. All contributors were informed at the point of participation that their input would inform a published report but that their individual identities would not be revealed. The thematic analysis presented in this report does not identify individuals, forces, or roles beyond broad categorisation.

Evidence Summary

What currently exists

Forces are generally aware of tech abuse as an issue, and many have recognised it as a strategic threat consistent with the NCVPP Strategic Threat and Risk Assessment. However, awareness tends to start from a low base, and the provision that does exist is characterised by significant variation across forces and roles.

Local and regional initiatives do exist, often driven by the personal commitment of dedicated digital and VAWG specialists, ranging from ad hoc advice and support provided by DMIs to frontline officers, to structured regional training programmes. There is also some awareness of specialist advice and support from partner agencies, though contributors report less clarity on when and how to access these services consistently.

Current gaps

At the time of writing, the picture across policing is of a fragmented and inconsistent response, with a number of structural gaps that have persisted over time:

- Victims and survivors of tech abuse often receive a patchy response, with significant variation between forces and individual officers.
- There is a persistent tendency to minimise online harms and prioritise physical forms of harm. This is compounded by recording practices that often capture only the primary offence type, meaning technology-facilitated abuse occurring within wider domestic abuse or stalking cases can be rendered invisible in police data.
- There is no systematic national horizon-scanning function to identify, assess and support policing to respond to emerging technology-enabled threats.
- While efforts are emerging internationally to articulate what an effective police response to technology-facilitated violence against women and girls (TFVAWG) should involve — including UN Women's Guidance for Police on Addressing Technology-Facilitated Violence Against Women and Girls (2025) — these provide high-level principles rather than the detailed operational guidance needed to support consistent frontline policing practice. There remains no comprehensive national operational guidance setting out what a good police response to technology-facilitated abuse should look like in England and Wales.
- There is no national community of practice through which police practitioners can develop expertise, share learning and good practice, and strengthen approaches to recognising and responding to technology-facilitated abuse.

Existing knowledge products

Awareness and uptake of the College of Policing Op Modify* package is low and uneven across forces, despite positive feedback from those who have engaged with it. Op Modify was developed in 2022 and has not been updated. Several contributors noted they were entirely unaware of its existence, while others, particularly those in cyber and digital specialist roles, described making it mandatory for their teams.

Beyond Op Modify, there is no national training or guidance on tech abuse generally. Tech abuse is not integrated into existing national VAWG training packages such as DA Matters. A small number of specific interventions exist, including work on deepfake image-based abuse and the Angiolini non-contact offences training package, but these are standalone and not embedded in a wider framework.

*Operation Modify (also known as Op Modify) is an online learning programme developed by the College of Policing to help new and serving officers, police staff and volunteers to acquire the digital skills they need to undertake investigations effectively. There are 15 episodes hosted on College Learn including a 'Digital spotlight on violence against women and girls (VAWG)' module

Thematic Findings from the Call for Input

The structured call for input generated rich evidence from across the policing workforce. The following presents key thematic findings drawn from that input. All contributions are presented in aggregate form only. No individuals, forces or specific organisations are identified. Five themes emerged consistently across contributors, regardless of force type, role or region.

> **A note on context.** The themes below document gaps and challenges that are consistent with findings from wider academic research, HMICFRS inspection evidence, and the testimony of victim and survivor services. They reflect both structural barriers, including the absence of national training, limited resourcing, and the pace of technological change, and cultural ones, including tendencies to minimise technology-facilitated harm or treat it as peripheral to core VAWG work. These patterns are not universal: this TNA also found real expertise, commitment and innovative practice across the contributor group.
>
> The purpose of naming challenges honestly is to support the case for the systemic change that would enable that good practice to become the norm.

Theme

UNDERSTANDING IS UNEVEN AND OFTEN SELF-TAUGHT

Understanding of tech abuse varied considerably across the contributor group, from sophisticated and detailed to limited or uncertain. What was particularly striking was how frequently those with stronger knowledge attributed this to personal research, professional self-motivation or the experience accumulated through specialist roles, rather than to any formal training provision. This pattern held regardless of whether contributors were frontline officers, investigators or digital specialists.

Contributors with detailed operational knowledge of tech abuse frequently noted they could not point to specific force or national provision that had produced that understanding. Where knowledge existed, it had typically been built through informal routes: engaging with third sector organisations, attending conferences in a personal capacity, or learning from colleagues on a case-by-case basis.

This creates a fragile capability base that is dependent on individual motivation and retention, rather than embedded organisational learning. When knowledgeable individuals leave or move roles, that capability frequently leaves with them.

Frontline contributors were the most likely to report limited understanding, with several noting that they would struggle to identify tech abuse as a distinct risk factor when responding to domestic abuse or stalking calls. This gap at first contact is significant, as it is the point at which digital safeguarding opportunities are most commonly missed.

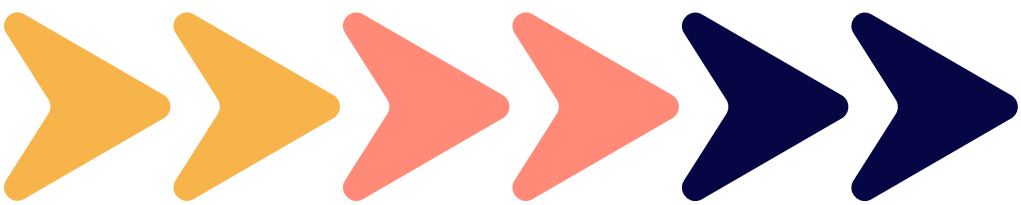
Theme

TECH ABUSE IS NOT YET TREATED AS CORE BUSINESS

Across the contributor group, there was consistent recognition that tech abuse is present and growing within the VAWG threat picture. There was, however, a parallel and equally consistent recognition that it is not yet treated as a core component of policing work. It tends to be positioned as an addition to existing offence categories rather than being integrated as a risk factor in its own right, within DA, stalking or coercive control responses.

This framing creates a systemic tendency to treat tech abuse as a specialist concern, which in practice can mean it is deprioritised or deferred to colleagues with cyber expertise, even in cases where the digital dimension is central to the harm being experienced. Contributors from public protection and VAWG roles described an ongoing challenge of advocating for tech abuse to be taken seriously at an organisational level, with progress often dependent on individual champions rather than structural change.

The absence of a mandatory national training requirement was frequently cited as a contributing factor to this dynamic. Where training is optional or confined to specialist teams, it reinforces the perception that tech abuse is a niche issue rather than something every officer responding to VAWG needs to understand.



3 Theme

TRAINING PROVISION IS ABSENT, FRAGMENTED OR OUT OF DATE

The picture of current training provision is strikingly consistent across contributors: structured, mandatory, force-wide training on tech abuse does not exist in most organisations. What does exist tends to be ad hoc, locally developed, or reliant on informal knowledge transfer from specialist colleagues. Several contributors noted that e-learning formats have low engagement and do not translate into practical capability, particularly for complex or fast-moving subject matter.

Where training does exist, it is frequently described as dated or overly generic, failing to keep pace with the rapid evolution of tech-facilitated harms. Contributors described investing significant personal effort in sourcing specialist content from organisations including national cybersecurity bodies and specialist domestic abuse organisations, often without organisational support, time allocation or recognition. The pace of technological change is a structural challenge: training packages risk becoming outdated before they are widely adopted, and there is currently no mechanism to ensure systematic updating.

Several contributors also noted that even where structured training exists, attendance can be low, particularly where it is not mandatory or where competing operational pressures make release for training difficult. This points to a delivery challenge as well as a content gap: training needs to be accessible, relevant and recognised as a priority within force cultures, not just made available.

4 Theme

EQUIPMENT AND RESOURCE GAPS COMPOUND TRAINING DEFICITS

Training gaps do not exist in isolation. Contributors from specialist and public protection roles frequently described resource constraints that limit the capacity to deliver an effective response even where knowledge and motivation are present. These include limited forensic capability, insufficient equipment to detect covert surveillance technologies such as tracking devices and hidden transmitters, inadequate specialist staffing, and significant delays in device examination that can affect evidence quality and victim safety.

A particularly consistent concern was the capability to identify and respond to covert tracking and monitoring devices in domestic contexts, which contributors identified as increasingly prevalent in stalking and domestic abuse cases. Specialist teams in a number of areas lack the equipment needed to sweep locations or detect active surveillance devices, limiting their ability to safeguard victims comprehensively.

Several contributors raised concerns about the loss of Digital Media Investigator (DMI) capability through resourcing pressures, with posts being reduced, merged with other roles or left unfilled. Where embedded DMI support has been lost, the impact on the quality of the tech abuse response available to public protection teams is direct and significant. Frontline officers without access to specialist digital support are less able to identify digital risk, preserve evidence or provide meaningful digital safeguarding advice to victims.

5 Theme
THERE IS STRONG APPETITE FOR A NATIONAL FRAMEWORK

Notwithstanding the challenges identified, contributors consistently expressed a strong appetite for change and clear views on what a better national framework would look like. The demand across roles and force types is not simply for more training in a generic sense, but for provision that is structured, practical, mandatory and regularly updated, and that treats tech abuse as a core element of policing VAWG rather than a specialist add-on.

There is strong support among contributors for a centrally coordinated national resource covering investigative guidance, emerging threat briefings, victim safeguarding advice and good practice case studies. Contributors also expressed a desire for clearer national direction on roles and responsibilities in tech abuse investigations, to address the current confusion about when and how to escalate, and who owns different elements of the response.

Contributors who have developed effective local or regional provision expressed strong support for their models being shared and scaled nationally. The interest generated by locally-developed programmes at national policing events, with multiple forces seeking to replicate successful approaches, illustrates the appetite that exists for evidence-based national leadership in this area.

What is Needed to Address Tech Abuse?

Effective policing responses require both the ability to identify tech abuse when it is occurring or has occurred, and the skills and knowledge necessary to respond appropriately, whether through investigative action, safeguarding, or both.

Operation Soteria is highlighted in the VAWG strategy as an example of good practice (Home Office, 2025). It is an evidence-based approach to addressing Rape and Serious Sexual Offences (RASSO) that is being implemented nationally following an in-depth academic review (Hohl & Stanko, 2022). Its National Operating Model (NOM) breaks down the journey from initial report to criminal justice outcome into structured stages with recommended good practice at each (National Police Chiefs' Council, 2025). Evidence suggests improvements in victim experience alongside reductions in case attrition (Victims Commissioner, 2024).

An effective strategy to address tech abuse must encompass three linked components: **identification of tech abuse; response to tech abuse; and integration into existing public protection and partnership responses.**

Identification of Tech Abuse

If tech abuse is to be effectively addressed, it must first be recognised. The landscape review found this was not happening consistently, from failures to record incidents accurately, to gaps in investigative response, to a persistent tendency to minimise survivor impact. Tech abuse includes a spectrum of behaviours: online harassment, digital stalking, surveillance via smart devices, account compromise, image-based abuse and misuse of social media platforms. Recognising these signs is a vital first step, particularly for frontline officers who are likely to be the first point of contact for victims.

CURRENT GAPS IN IDENTIFICATION CAPABILITY

- Limited awareness of evolving forms of tech abuse, including spyware, GPS tracking, smart home misuse and AI-facilitated harms
- Inability or unwillingness to identify subtle or hidden indicators of tech-enabled coercive control
- Limited understanding of how digital footprints and device data reveal patterns of abuse
- Gaps in recognising the disproportionate impact of tech abuse on particular groups, including those in high-risk DA situations

RECOMMENDED LEARNING FOR IDENTIFICATION

- Definitions and typologies of technology-facilitated abuse, illustrated by current trends and real case examples
- Practical exercises focused on identifying digital evidence and recognising indicators of tech abuse at first response
- Overview of risk assessment tools relevant to the digital context
- Awareness of how victim experience of tech abuse affects trust and confidence in policing

Responding to Tech Abuse

Once identified, an effective response is critical. Policing has considerable existing digital investigation capability at local, regional and national levels, but the focus of this capability on VAWG offences has been patchy. Digital investigation is a default approach in child sexual abuse and exploitation and serious organised crime; the same is not yet true for tech-enabled VAWG.

CURRENT GAPS IN RESPONSE CAPABILITY

- Limited expertise in identifying, securing, gathering and analysing digital evidence in the context of VAWG
- Lack of up-to-date training on relevant legal frameworks, including stalking, coercive control, image-based abuse and Computer Misuse Act Offences
- Insufficient victim-centred practice, particularly in digital safeguarding and device safety planning
- Challenges in working with technology companies and digital platforms to secure evidence and enable case resolution
- Lack of routine provision of digital safeguarding advice and support to victims at first contact

RECOMMENDED LEARNING FOR RESPONSE

- Digital investigation technique basics: device handling, evidence preservation and forensic awareness for non-specialists
- Legal frameworks: updated training on legislation relevant to technology-facilitated abuse
- Victim support: trauma-informed, intersectional approaches, digital safeguarding, account security and referral procedures
- Multi-agency working, including partnerships with technology firms, NGOs and victim services
- Scenario-based exercises to develop confidence in response decision-making

Integration into Public Protection and Partnership Responses

Tech abuse rarely occurs in isolation and is frequently part of a broader pattern of offending (Douglas et al, 2025; Home Office, 2025). Responses to tech abuse must therefore be integrated into wider VAWG and public protection frameworks (National Police Chiefs' Council, 2024). The Soteria principles (suspect-focused, victim-centred, context-led (Hohl & Stanko, 2022) are applicable to all forms of VAWG, including tech abuse, and should underpin an equivalent National Operating Model.

CURRENT GAPS IN PARTNERSHIP & PUBLIC PROTECTION INTEGRATION

- Tech abuse is not integrated into wider policing VAWG responses covering DA, stalking and harassment
- Tech abuse risk is not routinely considered within existing risk assessment processes, including MARAC arrangements
- No national operating model for addressing tech abuse currently exists

RECOMMENDED LEARNING FOR PUBLIC PROTECTION AND PARTNERSHIP

- Defining a partnership approach to recognising tech abuse within existing inter-agency risk assessment and public protection systems
- Practical guidance and support on digital risk assessment in MARAC* and MAPPA* contexts
- Partner engagement on developing shared identification and response knowledge
- Horizon scanning for future threats in partnership with academic, third sector and industry partners, who hold TFVAWG / online safety expertise.

Continuous Professional Development

Tech abuse is a dynamic and rapidly evolving threat. Continuous professional development (CPD) for officers, staff and partner agencies is not an optional enhancement, it is a structural requirement. This must encompass regular refresher training on both identification and response, systematic tracking of technological trends, and mechanisms for sharing practice and learning from casework.

There are useful parallels with the CPD infrastructure developed around other fast-moving threat types: the role of Team Cyber UK in building a sustainable response to Computer Misuse Act offences, or Operation Hydrant in sustaining CPD for Child Sexual Abuse & Exploitation (CSAE) investigators, both illustrate what is achievable with appropriate national investment and coordination. Ensuring that a national operating model for tech abuse encompasses both horizon scanning and CPD is a clear and immediate priority.

**MARAC (Multi-Agency Risk Assessment Conference): a multi-agency meeting where police, health, housing, probation, specialist domestic abuse services and other agencies share information and coordinate responses to the highest-risk domestic abuse cases.*

**MAPPA (Multi-Agency Public Protection Arrangements): a framework through which police, probation and other agencies share information and work together to assess and manage individuals who pose a risk of serious harm to the public.*

Case Study Yorkshire & Humber ROCU: Regional Tech Abuse Training Programme

Yorkshire and Humber regional organised crime unit (YHROCU) has developed and delivered a comprehensive tech abuse training programme, demonstrating what can be achieved through a coordinated regional approach. At the time of writing, the programme has been delivered to approximately 2,000 police officers and staff and 1,000 partner agency staff across multiple forces in the region, as well as domestic abuse services and local authority staff.

The programme consists of a 90-minute workshop delivered in person or online, via the regional cyber protect network. Content covers:

- Relevant legislation, including DA, stalking, Computer Misuse Act offences and new image-based abuse offences
- Practical examples of how perpetrators use technology to commit abuse
- Features common in stalkerware, including misuse of consumer-facing tracking apps
- How to identify and respond to different forms of tech abuse
- Cyber protect advice on securing technology for victims
- The role of connected devices (IoT) in the home environment economic abuse facilitated by technology
- The rise of deepfakes and AI-facilitated abuse
- Links to third-party resources including national cybersecurity guidance, specialist domestic abuse organisations and online safety resources

For police officers and staff, content also includes identifying and preserving digital evidence and how to access specialist support including digital forensics. A number of victim and survivor clinics have been delivered across the region in partnership with local agencies, offering hands-on support with checking devices for stalkerware and enabling security features.

The programme has independently been evaluated by academic researchers at the University of Sheffield. It represents a compelling example of what regionally co-ordinated, specialist-led, practically-focused provision can achieve, and a strong candidate for national scaling under NCVPP coordination.

Annex A: Stakeholder Consultation Methodology and Summary Findings

A structured call for input was circulated across police forces in support of this TNA between January and April 2026. Responses were received from 40 officers and staff from approximately 20 forces and policing organisations, including national policing bodies, regional organised crime units, and a range of forces. Contributors were informed that their input would inform a published report but that their identities would not be revealed.

The following summarises the key themes arising from the stakeholder consultation, based on analysis of responses across all 12 question areas. All responses are presented in aggregate form only. No individual, force or organisation is identified.

Understanding of tech abuse

Understanding varied across the contributor group, from detailed operational knowledge to limited familiarity. More experienced contributors and those in specialist roles tended to provide richer accounts, encompassing digital coercive control, surveillance technologies, account compromise and AI-enabled harms. Frontline contributors were more likely to define tech abuse narrowly, for example in terms of social media harassment or image-based abuse, and less likely to identify it as a pattern embedded in wider abuse. Several frontline respondents indicated limited or no understanding. Across the group, the definition of tech abuse as a distinct and named phenomenon was less well established than awareness of the individual offence types it encompasses.

Tech abuse in force VAWG threat assessments

The majority of contributors were able to confirm that tech abuse features within their force VAWG threat assessment or control strategy, either as an explicit strand or embedded within stalking, harassment or DA categories. However, several contributors, particularly from frontline and non-specialist roles, were unaware of how or whether tech abuse featured in force strategic documents. A recurring observation was that even where tech abuse is recognised strategically, this recognition does not reliably translate into operational practice or training provision.

Tracking emerging threats

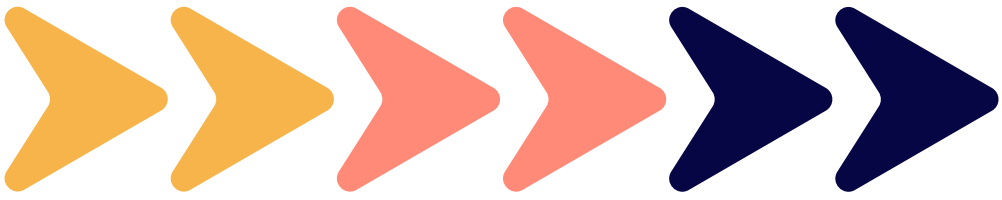
Emerging threat tracking is primarily conducted at a national level through NPCC channels, College of Policing networks (including DIAG) and regional structures such as ROCUs. At the force level, this is supplemented by local intelligence systems, keyword searches and crime report scanning, though this tends to be the work of specialist teams rather than a systematic force-wide capability. The majority of contributors, particularly those in frontline or non-specialist roles, had no awareness of how emerging threats were tracked in their organisation and relied on national intelligence products, media monitoring or individual CPD. Deepfake AI abuse and stalkerware were consistently identified as threat areas where capability is lagging behind the threat.

Current training provision

The consistent picture is of very limited structured training at force level. Where training does exist, it tends to be ad hoc, locally developed, and not embedded in mandatory force-wide provision. A small number of forces have more developed local offerings, often built around specialist cyber or VAWG teams. The most commonly referenced formal provision was the College of Policing Op Modify e- learning package, though awareness of this was uneven. Several contributors from specialist and public protection roles described investing significant personal time in sourcing training from external organisations. Frontline contributors were most likely to report having no training at all.

Awareness of Op Modify

Awareness of the Op Modify tech abuse module was mixed. Those in cyber, digital investigation and specialist VAWG roles tended to be more aware of it, with some describing it as mandatory within their own teams. However, a significant proportion of contributors, particularly those in frontline, DA and public protection roles, were unaware of the module, and some were unaware that a tech abuse component within Op Modify existed. Where Op Modify had been accessed, feedback was generally positive. Concerns were raised about the currency of the content and whether it reflects current threat types, and about uptake being left to individual discretion rather than mandated.



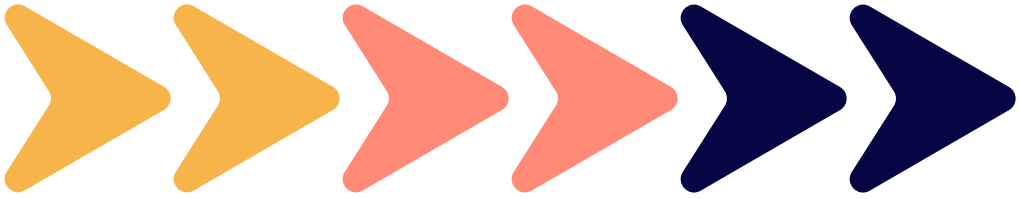
Digital Media Investigators and specialist digital support

The majority of forces represented in the contributor group have DMI or DTAC (Digital Technology and Communications) capability. However, the level of integration between this capability and public protection teams varies considerably. In several forces, DMI support is embedded and actively accessed by frontline and DA officers. In others, it is prioritised for high-harm or complex cases and less routinely accessible. A small number of contributors reported that their force had recently lost full-time DMI capability due to resourcing pressures. The loss of embedded specialist digital support was consistently described as a significant gap in the ability to deliver a proportionate tech abuse response.

Key gaps identified by contributors

The training needs and capability gaps most frequently identified by contributors were:

- Lack of structured, mandatory, force-wide frontline training on tech abuse recognition and response
- Limited awareness of digital lines of enquiry and failure to treat digital evidence gathering as a first-response priority
- No consistent referral pathway to specialist support
- Equipment gaps, particularly around covert surveillance device detection Insufficient capacity to process digital evidence quickly
- Lack of national guidance and shared good practice
- Confusion about roles and responsibilities in tech abuse investigations Inconsistent advice to victims, including concerns about misleading guidance from non-specialist sources



What training contributors want to see

Contributors were consistent in their views on what training provision should look like:

- Practical, scenario-based frontline training covering recognition and first response to tech abuse
- A structured 'digital golden hour' framework, akin to physical lines of enquiry, setting out what actions should be taken at first contact
- Mandatory force-wide delivery, not restricted to specialists or delivered solely via e-learning
- Regular updates to keep pace with emerging technologies
- Bespoke specialist training for investigators and DMIs on emerging threats including AI-generated content and deepfakes
- A national centralised repository of good practice, case studies, investigative checklists and emerging threat briefings
- Clearer links between policing and specialist third sector organisations to ensure their research and best practice informs training development

Selected References:

- Douglas, H., Tanczer, L., McLachlan, F., & Harris, B. (2025). Policing technology-facilitated domestic abuse (TFDA): Views of service providers in Australia and the United Kingdom. Journal of Family Violence, 40, 341–352. https://doi.org/10.1007/s10896-023-00619-2
- Herdale, G., Duddin, K., & Jurasz, O. (2025). Landscape Review: The Police Response to Technology-Facilitated Abuse. Centre for Protecting Women Online, The Open University.
- Hohl, K., & Stanko, E. A. (2022). Five pillars: A framework for transforming the police response to rape and sexual assault. International Criminology, 2(3), 222–229. https://doi.org/10.1007/s43576-022-00057-y
- Home Office. (2025). Freedom from Violence and Abuse: A Cross-Government Strategy to Build a Safer Society for Women and Girls. Volume 1: Strategy. Home Office.
- National Crime Agency. (2026). National Strategic Assessment 2026.
- National Police Chiefs' Council. (2024). Violence Against Women and Girls Strategic Threat and Risk Assessment. National Police Chiefs' Council.
- National Police Chiefs' Council. (2025). Operation Soteria – Transforming the Investigation of Rape. National Police Chiefs' Council.
- National Police Chiefs' Council, & College of Policing. (2024). Violence Against Women and Girls National Policing Statement. National Police Chiefs' Council & College of Policing.
- Office for National Statistics. (2025). Domestic abuse prevalence and trends, England and Wales: Year ending March 2025. Office for National Statistics.
- Refuge. (2025). Technology-Facilitated Abuse Service Annual Data 2025. Refuge.
- Refuge (2026) 'Refuge exposes alarming new patterns of abuse involving wearable technology'. Available at: Refuge (Accessed: 1 September 2026).
- Sondhi, A., Harding, R., Maguire, L., & Williams, E. (2023). Understanding factors associated with burnout symptoms amongst investigators working on rape and serious sexual offence (RASSO) investigations in England and Wales. Policing: A Journal of Policy and Practice, 17, paad020. https://doi.org/10.1093/police/paad020
- Sondhi, A., Harding, R., & Williams, E. (2025). Segmenting the rape and serious sexual offence (RASSO) investigator workforce: Implications for wellbeing and burnout. Police Practice and Research, 26(3), 312–324. https://doi.org/10.1080/15614263.2024.2426172
- Victims' Commissioner for England and Wales. (2024). Operation Soteria: Improved victim experiences encouraging, but real areas of concern remain. Victims' Commissioner for England and Wales.
- UN Women (2025) Guidance for police on addressing technology-facilitated violence against women and girls. New York: UN Women. Available at: UN Women guidance (Accessed: 31 August 2026).

Centre for Protecting Women Online

Training Needs Analysis

September 2026

The Open University, Milton Keynes, UK

Email: protecting-women-online@open.ac.uk