NCVPP

National Centre for Violence Against Women & Girls and Public Protection

Using the Experience of Victim/Survivors to Improve Police Practice

Stage 4 - Managing Information

December 2025

College of Policing

NPCC National Police Chiefs' Council

Contents

Executive Summary

- Consider the most appropriate method for recording information from engagement practices. Extra consideration may be required for feedback that may have legal implications.
- Data must be stored securely and in compliance with the relevant legal standards. Formal policies should be in place to protect the privacy of victim/survivors.
- Data retention should follow force policy, balancing analysis needs with privacy.
- Individuals can request deletion of their personal, identifiable information at any time. They may also withdraw consent for their contributions to be included in the findings, though this is not always possible outside of agreed timescales.
- Individuals should be informed of their rights around retracting data. This can be communicated through privacy notices and can help build trust and ensures transparency.
- Formal retraction policies should be established to uphold the rights of those involved in the engagement practice.

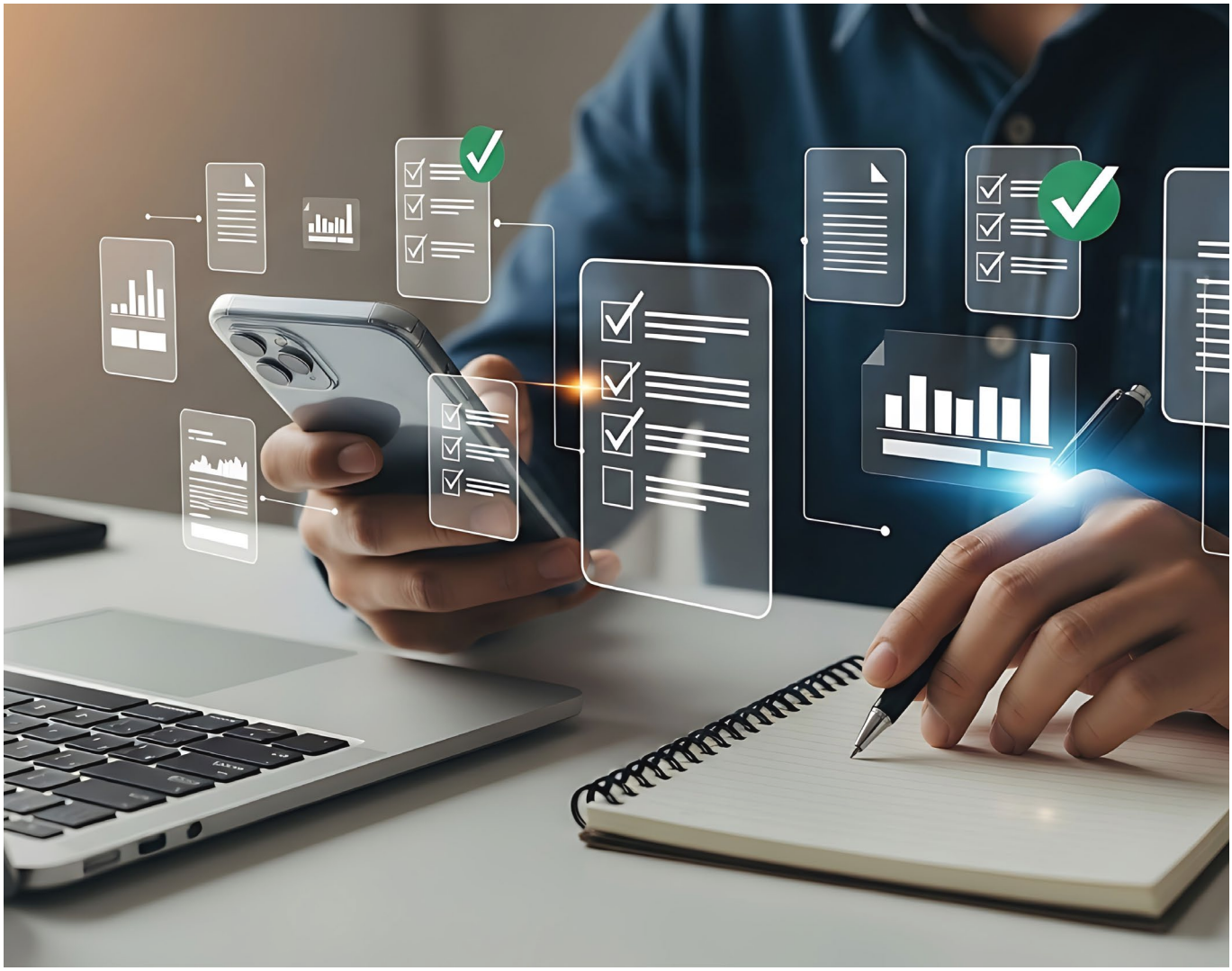
4.1 Guidance and Legislation

It is important to record, store and retain information provided about individuals involved the engagement practices appropriately. Secure handling of information is an ethical obligation to victim/survivors. Processes for managing information collected through engagement practices should also comply with statutory guidance, legislation, and force policies at all stages. This ensures that data is held lawfully, ethically, and transparently.

Relevant guidance and legislation includes:

- General Data Protection Regulation (GDPR): Legislation regarding data privacy and security.
- Data Protection Act 2018: Legislation outlining standards for protecting personal data in accordance with recent EU data protection laws.
- Police Information and Records Management Code of Practice: Statutory Code of Practice and guidance setting national principles for police information and records management.

Officers/staff involved with the engagement practice should consult with the relevant data protection and information management teams at all stages. This ensures that information is managed correctly from the start of the practice and that data is not held for longer than necessary.



4.2 Recording Data/ Information

Generally, two types of data or information are recorded during an engagement practice. This can be information relating to the victim/survivor's identity, or information relating to their experiences e.g. their feedback or responses.

- **Feedback/responses:** Refers to the information provided by an individual about their thoughts and experiences in relation to the aims and purpose of the engagement practice.
- **Personal data:** This is defined in GDPR as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'. Under GDPR, the sharing of any personal data (data which relates to an identifiable individual) requires a lawful basis, which is outlined in Article 6, unless it falls into a special category data, outlined in Article 9.

There are various methods for recording information from engagement practices. Consider which recording method is most appropriate. For example, digitally recording responses may be more appropriate for large surveys whereas taking meeting notes may be more appropriate for verbal feedback in small groups.

In some cases, it may be appropriate to give extra consideration about which method is most appropriate, such as when victim/survivors are sharing information that could have legal implications. In these circumstances, appropriate methods could include capturing feedback through reflections following the engagement or capturing specific actions and suggestions whilst removing details about individual cases. This can help enable a more naturalistic and comfortable listening environment and prevent potential legal implications for those in attendance. For more considerations about safeguarding victim/survivors involved in engagement practices, see Stage 3.

Officers/staff should be aware of how to accurately record information in line with force policy and should consult with the relevant data protection and information management teams. This can include advice on relevant policies, guidelines and legislation, or any additional training/upskilling that may be useful.

4.3 Storing Data/Information

4.3.2 How should data/ information be stored?

To ensure the secure and effective storage of data (both digital and non-digital) from voice of the victim/survivor (VoV/S) practices, officers/ staff should consult their force data policies and data protection teams. This should ensure that the data is held in line with GDPR (Art 6 & 9), Data Protection Act 2018 (Ch 2) and other relevant legal requirements. This is especially important within the context of collecting victim/survivor responses, owing to the personal and sensitive nature of the information obtained. Data storage practices should include:

- **Adherence to legal and contractual standards -** Implement formal policies that dictate how victim/survivor data is stored, shared, and accessed, ensuring compliance with all relevant regulations.
- **Data flows -** Understand how data will be used, who will have access to it and when. For example, if sharing data with external agencies, ensure that email chains have been appropriately stored or deleted in line with force policies.
- **Secure digital storage systems** - Utilise encrypted systems, secure emails, and password-protected folders to store sensitive information. Regularly review who has access to the data and ensure permissions are kept up to date.
- **Secure non-digital storage systems -** Ensure any data kept in non-digital formats, such as written notes, is stored in line with force data policies. Regularly review who has access to the data and ensure physical access (e.g. through key fobs or key cards) is regularly updated.
- **Anonymisation -** In a lot of cases, it will be most appropriate to anonymise personally identifiable data before analysis to protect victim/survivor identities. Where anonymisation is not possible, consider using pseudonyms instead.
- **External agencies -** External agencies that are commissioned by forces to engage with victim/survivors should have formal contracts in place to ensure any recorded data is securely stored, shared and only accessible to personnel with clearance.

4.3.2 How long should forces keep data/information?

Data retention periods can vary, but they should be tailored to the nature of the data, its purpose, and adhere to force policy. It is important to develop protocols for securely disposing both digital data and non-digital data. It is important not to keep information for longer than purposes of processing require. Practices should include:

- **Alignment of retention periods -** Consult relevant force policies, force subject matter experts and data protection teams. Ensure data is being held in line with legal requirements and national guidelines.
- **Development of formal contracts -** External agencies that are commissioned by forces to engage with victim/ survivors should have formal contracts in place to specify how long they may retain identifiable data for different circumstances.

4.3.3 Retraction of data/ information

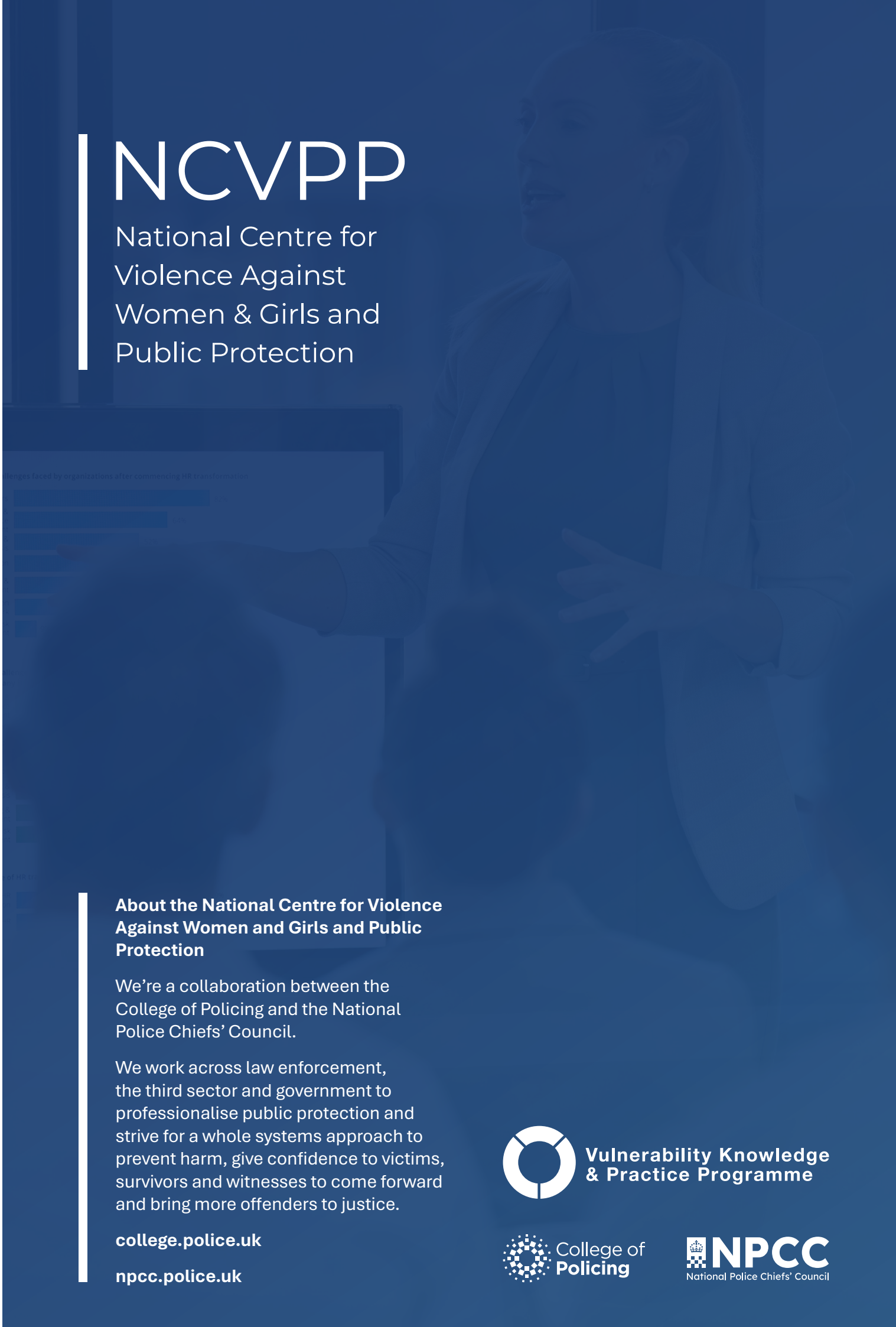
Individuals have the right to request that data be deleted if they withdraw their consent or change their opinion on the information they provide, without giving a reason. They should be informed of this during initial engagement (see Stage 2). Allowing for feedback to be retracted ensures that data collection processes are both accurate and ethical. Considerations for practice include:

- **Implementing formal retraction policies:** Individuals must be informed of their right to request their information to be deleted if they withdraw consent or change their opinion. Establishing formal procedures for retraction can help improve consistency between forces, uphold individuals' rights under GDPR, build trust, and ensure feedback collection is both accurate and transparent.
- **Transparency:** There may be challenges in retracting information following engagement. For example, the information may already have been included in findings, the data may have been anonymised, or the information may have been deleted in line with legal requirements and force data retention policies. Individuals should be informed of any relevant timeframes for withdrawing their consent to ensure transparency and allow informed decision making. However, personal/identifiable information can always be retracted in line with GDPR. Consider the use of privacy notices to inform victim/survivors involved in the engagement practice about their individual rights.
- **Understanding reasons for retraction:** It is important to recognise the value of understanding why individuals may choose to withdraw their contributions. Where feasible, gathering this information can provide valuable insights into areas for service improvement and help identify potential barriers to building trust with victim/survivors. However, it is important to capture overarching reasons rather than collecting more details about an individual who is already in the process of retracting their information.

Overall, it is essential to establish clear governance policies and processes on data protection and information management to ensure compliance with force policies. This will help safeguard sensitive information and maintain trust in data handling practices.

Glossary

Term	Description
Good Practice	Practice referred to as 'good practice' reflects positive processes, approaches and useful resources. This is intended to provide examples that could be considered by forces but may not have been evaluated.
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". (GDPR, 2016)
Independent Advisory Groups (IAGs)	Independent Advisory Groups (IAGs) are a network of individuals independent of the Police who meet to advise and offer ideas to police forces on a wide range of activities relating to local policing.
Victim/survivor	Those who have been subject to, or have witnessed, a vulnerability related crime. The term represents a continuum upon which people may find themselves, in recognition of the fact that people with lived experience of victimisation may prefer one term or the other, and each journey from 'victim' to 'survivor' is unique.
Voice	The term 'voice' covers both the verbal articulation of wishes, experiences, and needs, alongside non-verbal indicators and features of the individuals' context, environment, and relationships. Voice not only means capturing and recording wishes, experiences, and needs, but also listening to and considering voices to influence and inform decision making.
Voice of the Victim/ Survivor (VoV/S)	'Voice of the victim/survivor' refers to the perspective of individuals (adults and children) who have been impacted by crime or harm: either through lived experience, as a witness, family member, friend or colleague. The perspectives, opinions, rights and non-verbal cues of victim/survivors and their advocates must be heard, respected, prioritised and actively sought during investigations, enquiries and interactions. They must also be embedded within policy, practice, and support provision. In turn, this will aid in strengthening investigations, shaping and developing current and future policy, practice, response and support of policing and wider agencies to victim/survivors, for those who need support.
VoV/S Practice	A Voice of the Victim/survivor Practice refers to any engagement process through which agencies collect feedback from or collaborate with victim/ survivors to gain insights into their perspectives, experiences, and rights. The information gathered should be used to inform future discussions, enhance responses, and strengthen practices moving forward.



NCVPP

National Centre for Violence Against Women & Girls and Public Protection

About the National Centre for Violence Against Women and Girls and Public Protection

We're a collaboration between the College of Policing and the National Police Chiefs' Council.

We work across law enforcement, the third sector and government to professionalise public protection and strive for a whole systems approach to prevent harm, give confidence to victims, survivors and witnesses to come forward and bring more offenders to justice.

college.police.uk

npcc.police.uk

Vulnerability Knowledge & Practice Programme

College of Policing

NPCC National Police Chiefs' Council