# **Policy Document**



#### **CYBER CRIME**

Version 4

#### 1. Policy statement

The rapid development of digital technology and the internet in recent years has provided criminals with new opportunities to commit crime across the world and across borders. Such crimes have just as damaging an impact on victims as if they had happened in the physical world and they are being perpetrated and reported at an ever increasing rate. According to the national lead on cybercrime, over half of all UK crime is now on line<sup>1</sup>.

As criminals find new and innovative ways to use technology and the internet it is essential that the Police Service has the resources necessary to prevent, investigate and to protect members of the public from the harm such crime causes. This includes the provision of training for police officers to ensure they have the skills and knowledge to confidently use digital technology in the prevention and detection of cyber related crime.

#### 2. Responsibility

The National Board is responsible for all policy formation.

### 3. Summary

Eighty per cent of adults in the UK now regularly use the internet. Many children suffer cyber bullying and a recent Fraudscape report has identified that those aged over 60 are the most vulnerable to cyber fraud. The rapid development of digital technology and the internet in the last 20 years has created new opportunities for criminals to perpetrate crimes against victims. PFEW believes that the Service needs to develop a clear understanding on the impact on demand for police services, as digital technology and the internet is increasingly used to perpetrate crime, so that the service provided to the public, including victims, can be improved.

PFEW believes that it is essential that police officers have the skills to deal confidently with digital technology; many crimes require some form of digital investigation whether or not the crime was committed on line. Chief Constables and Police and Crime Commissioners must ensure that all officers are provided with the necessary training on the use of digital technology to develop their skills and knowledge to tackle cybercrime. Worryingly, HMIC has identified that 'very few forces are

<sup>&</sup>lt;sup>1</sup> DCC Peter Goodman, national lead on cybercrime, PFEW National Detectives Forum, October 2016

focussing on developing the digital skills of their officers and staff despite a universal acceptance that digital skills are an increasingly important part of police work'<sup>2</sup>

## 4. Procedures/implementation

PFEW will press the National Police Chiefs Council, the Association of Police and Crime Commissioners and the College of Policing "to focus on protecting people from this type of harm through the development of new tactics and capabilities"<sup>3</sup>

PFEW will press the National Police Chiefs Council, the Association of Police and Crime Commissioners and the College of Policing to ensure that all officers are provided with training on the use of digital technology to improve the investigation and detection of cyber related crimes.

Responsibility is delegated to the National Secretary and/or the appropriate sub-committee.

|           | Author | Date         | Date to be reviewed | Change   |
|-----------|--------|--------------|---------------------|--|
| Version I | EP-KP  | June 2015    | June 2016           |  |
| Version 2 | KP-EP  | June 2016    | June 2017           | No change  |
| Version 3 | KP-EP  | June 2017    | June 2018           | Inserted references to HMIC State of Policing report 2016 & Policing Vision 2025 |
| Version 4 | KP     | January 2019 | June 2020           | Minor changes  |

## Signed by:

National Chair

National Secretary

<sup>3</sup> Policing Vision 2025

<sup>&</sup>lt;sup>2</sup> HMIC State of Policing: The Annual Assessment of Policing in England and Wales 2016