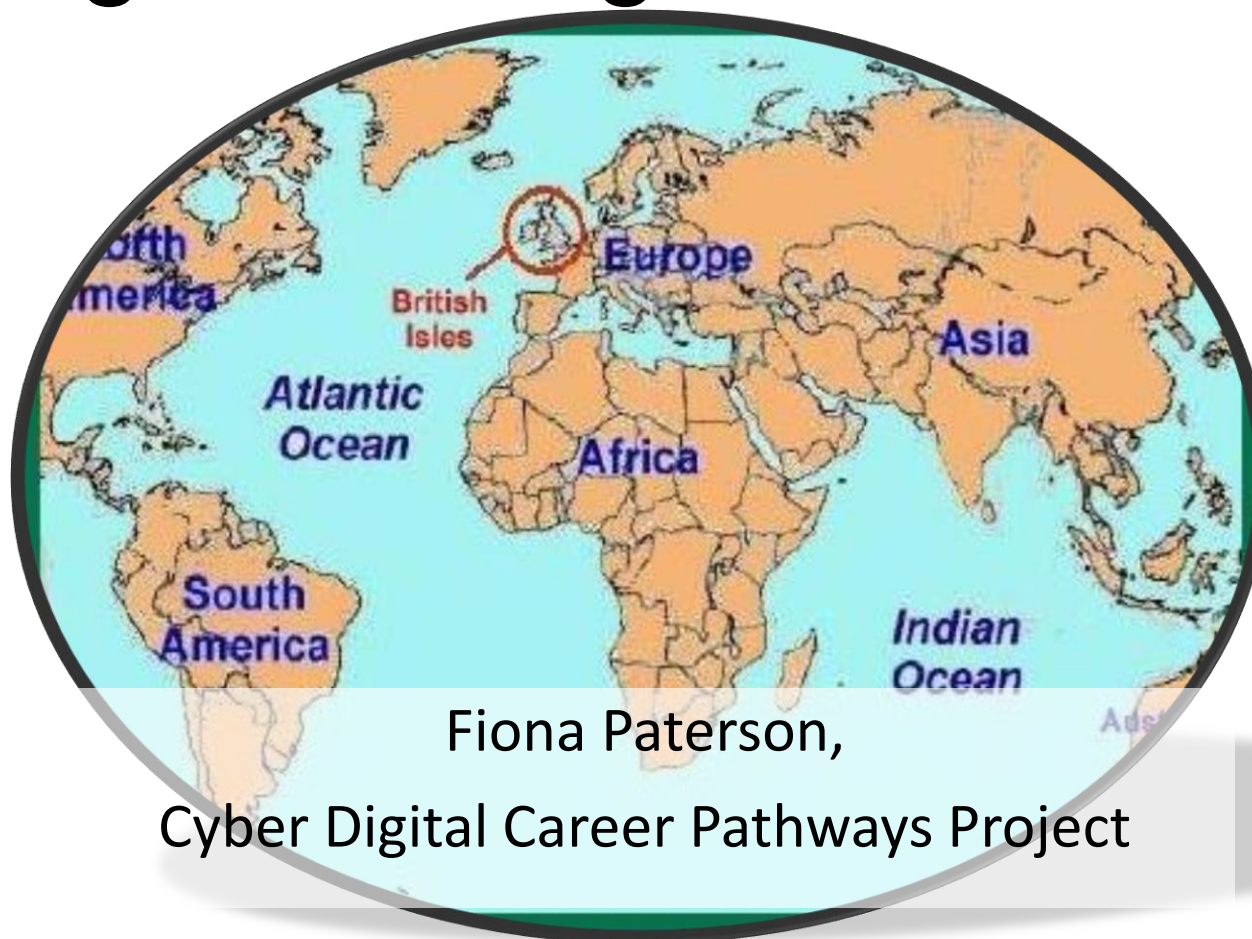


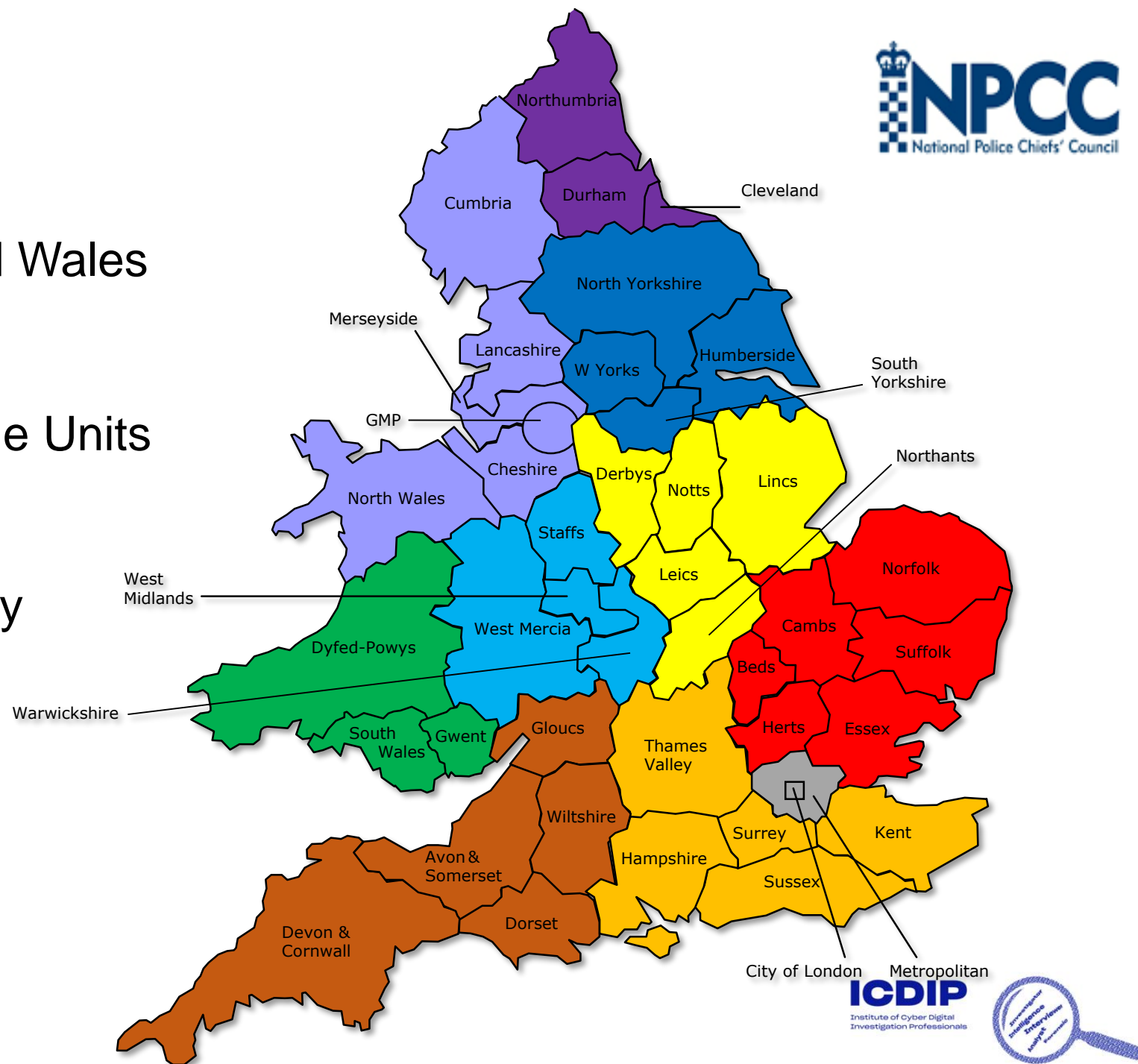
Cyber and Digital Training Strategies in England and Wales



Fiona Paterson,
Cyber Digital Career Pathways Project

Police structure in England and Wales

- 43 Local police forces
- 10 Regional Organised Crime Units
- 1 National Crime Agency
- Mainly operate independently



ICDIP

Institute of Cyber Digital
Investigation Professionals

The Professionalisation of Cyber Digital Investigations

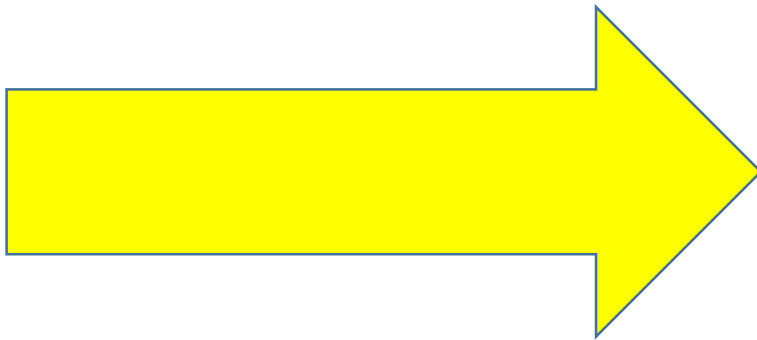


Project, History & Rationale:

- Outcomes of Government meeting September 2015
- Retention - 'Churn' ?
- Credibility at court - No current professional 'level'
- Solution for all Law Enforcement at the heart of cyber digital investigations



Starting Point



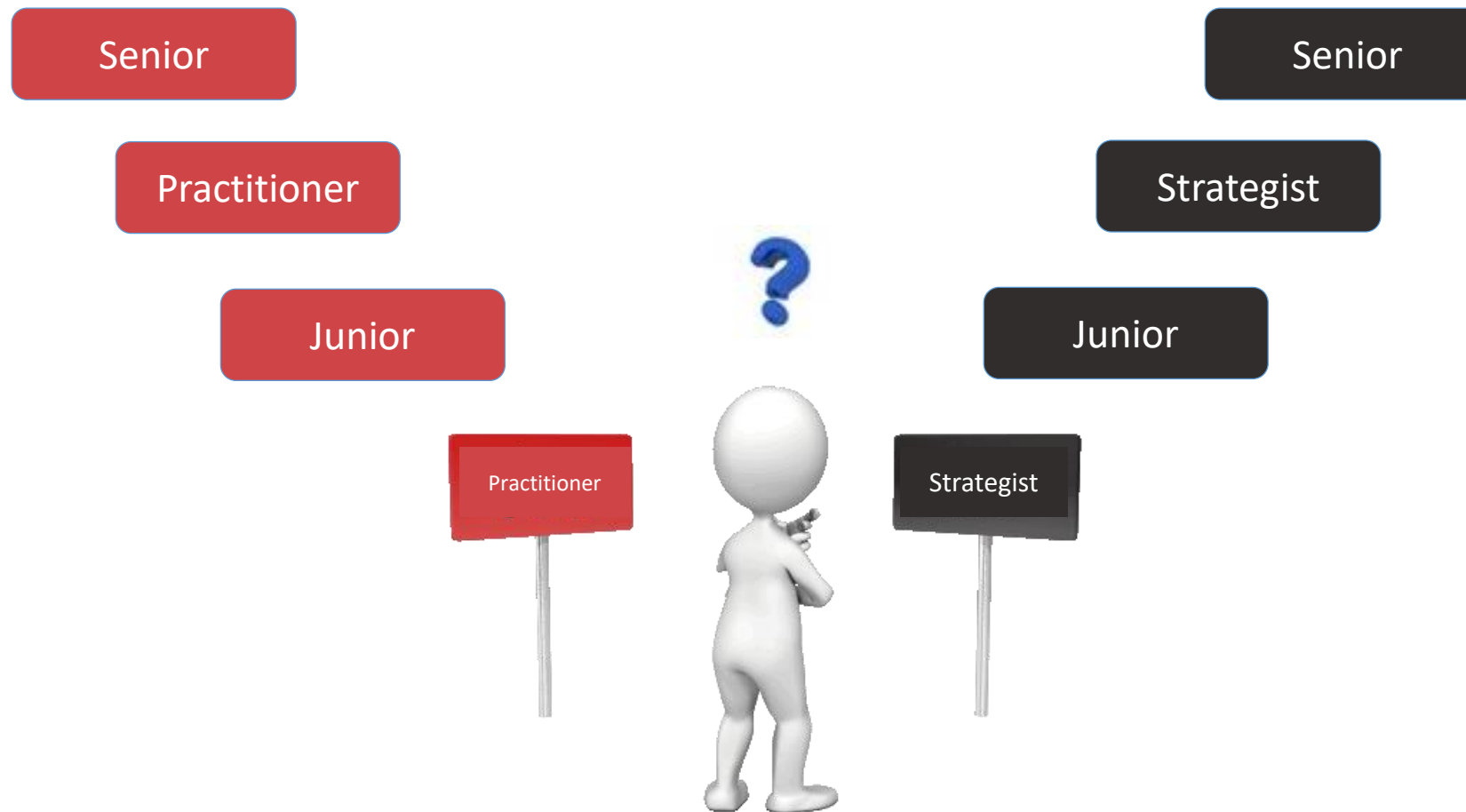
The Project Since 2016

Scoped the need for Investigation Skills Framework AND delivered:

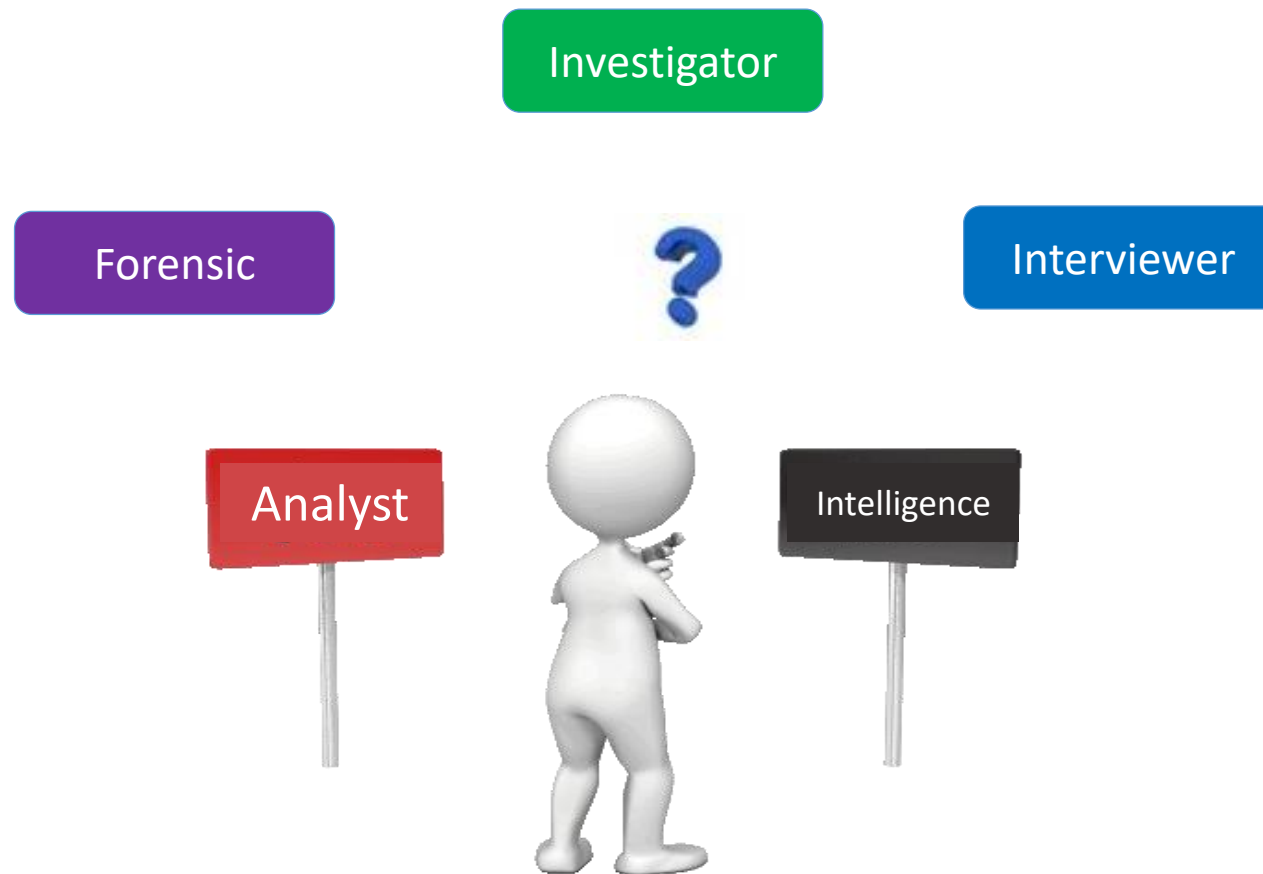
- CDCP Skills and Standards Framework©
- Professional status for:
 - **Investigators – Intelligence – Forensics - Analysts - Interviewers**
- National Register of Cyber/Digital Training Excellence (NRCDTE)
- Candidate Assessment processes
- Awards of industry standard professional status and membership of ICDIP
- CDCP Succession Plan – Condition of continued professional status



Application process:



Applying: Which job family?





© College of Policing Limited (2018) All rights reserved.

No part of this publication may be reproduced, modified, amended, stored in any retrieval system or transmitted, in any form or by any means, without the prior written permission of the College or as expressly permitted by law. Anyone wishing to copy or re-use all or part of this publication for purposes other than expressly permitted by law must be done under licence. Licence applications can be sent to Diane Kennedy, Intellectual Property Rights (IPR) and Licensing Manager, email diane.kennedy@college.pnn.police.uk Where we have identified any third-party copyright material you will need permission from the copyright holders concerned. Any other enquiries regarding this publication please contact us at contactus@college.pnn.police.uk or on 0800 4963322. This document has been created with the intention of making the content accessible to the widest range of people regardless of disability or impairment. To enquire about having this document provided in an alternative format please email contactus@college.pnn.police.uk



© Copyright College of Policing (2018).
All rights reserved.

Cyber Digital Investigation Profession Skills and Standards Framework for 'Law Enforcement Staff at the core of Cyber Digital investigations, who may have to present evidence at court on their Specialist Cyber Digital Investigation Skills'

Investigator - Subject Practitioner

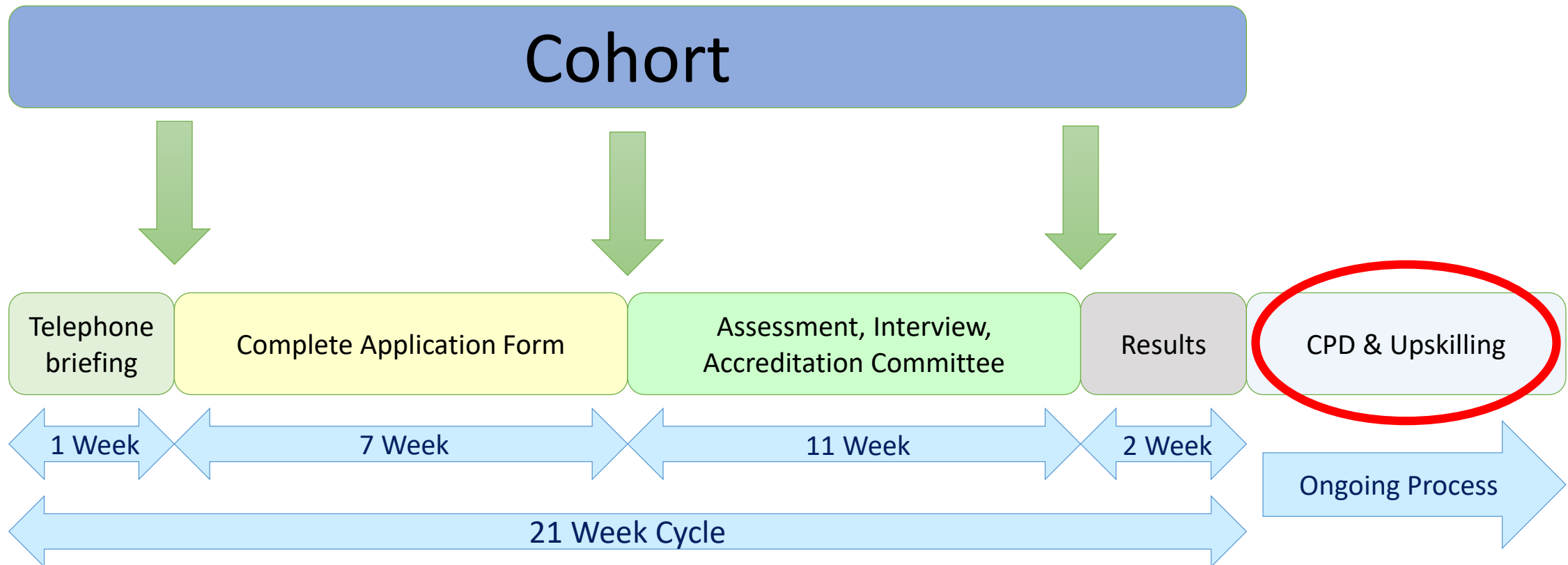
Person competent in cyber digital investigative skills and their practical application. Demonstrates effective investigative and intelligence techniques and the production and management of associated case files and documentation. Has an ability to work independently whilst also helping teams to apply policy/processes as part of an investigation. Has an ability to develop, propose, apply and demonstrate new processes, practices and measure performance outcomes.

Core (C) & Essential (E)

Skill Ref No.	Skill Group	Skill Title		
CDP205	Conducting Investigations	First Response	Demonstrates and applies understanding of how to take first response actions in investigations involving cyber digital related evidence.	E
CDP402	Conducting Investigations	Conduct Cyber Digital Investigations	Demonstrates the ability to conduct cyber digital investigations.	E
CDP459	Conducting Investigations	Investigating electronic evidence	Demonstrates the ability to apply practices to investigate electronic evidence.	E
CDP003	Personal and Managerial Effectiveness	Stakeholder Engagement	Demonstrates the ability to work and network with stakeholders to quantify and improve service delivery and progress shared objectives and interests in relation to cyber digital investigations	C
CDP012	Personal and Managerial Effectiveness	Communication and Knowledge Sharing	Proactively recognises, produces and shares good practice, and advice with colleagues and contributes effectively to debates and complex discussion demonstrating well-reasoned and measured arguments and conclusions.	C



Application Process 2019/20:

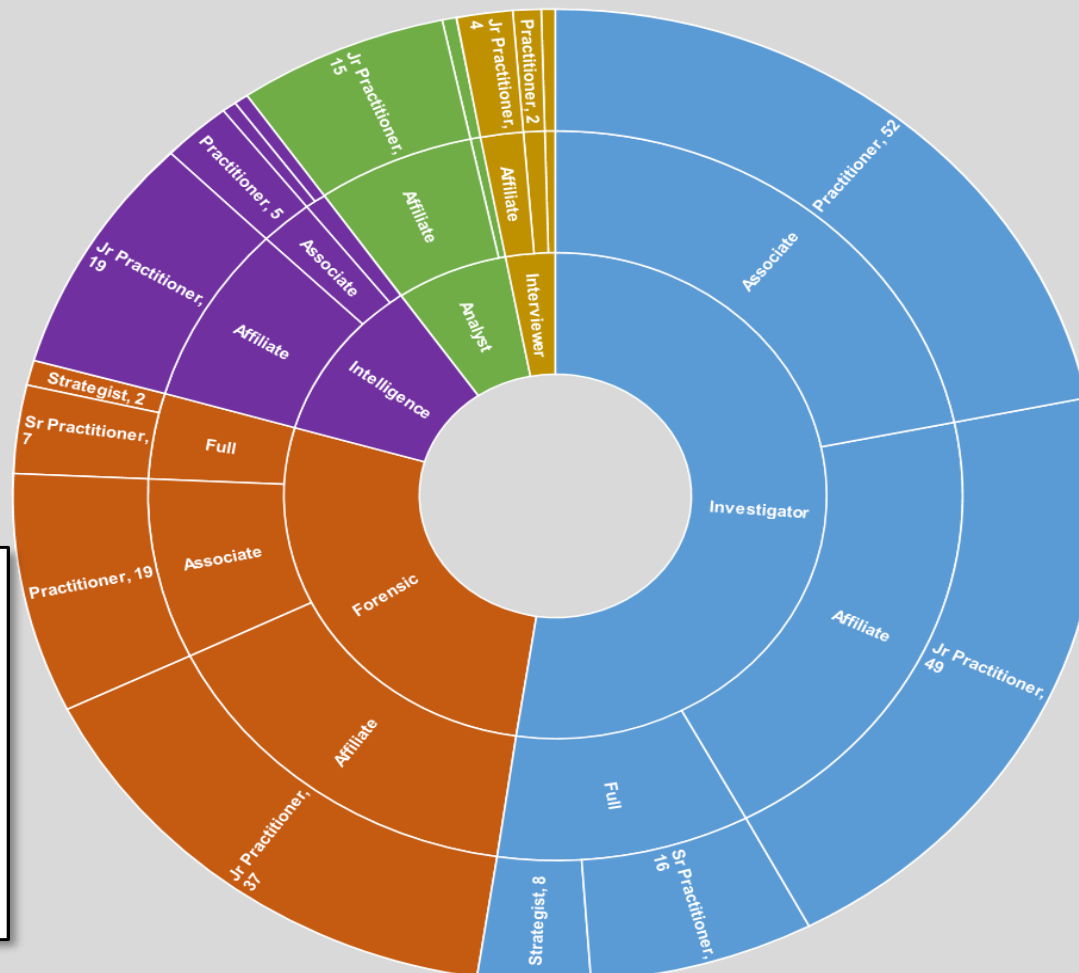


Current ICDIP membership breakdown

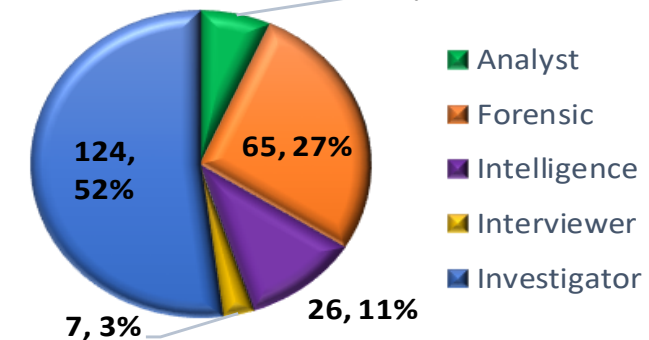
Total Membership
244

Total LE agencies
40

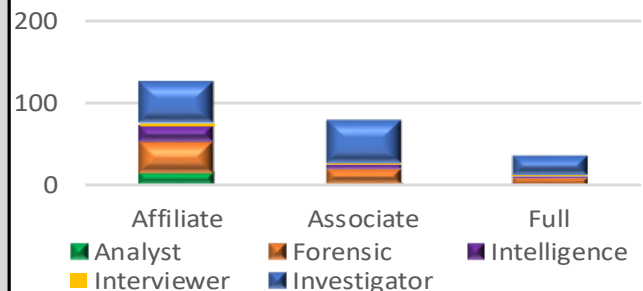
Upskilling opportunities
165



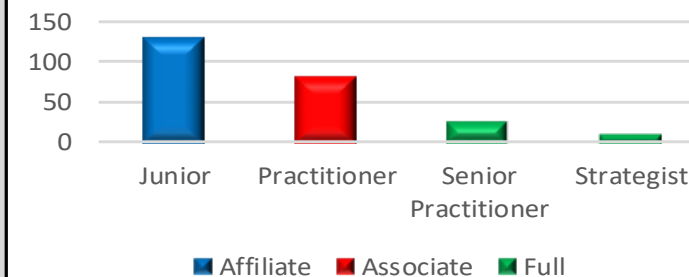
Job family breakdown



Breakdown by membership level



Breakdown by practitioner level



99%
See CDCP as
positive step

87%
Satisfied with
scheme

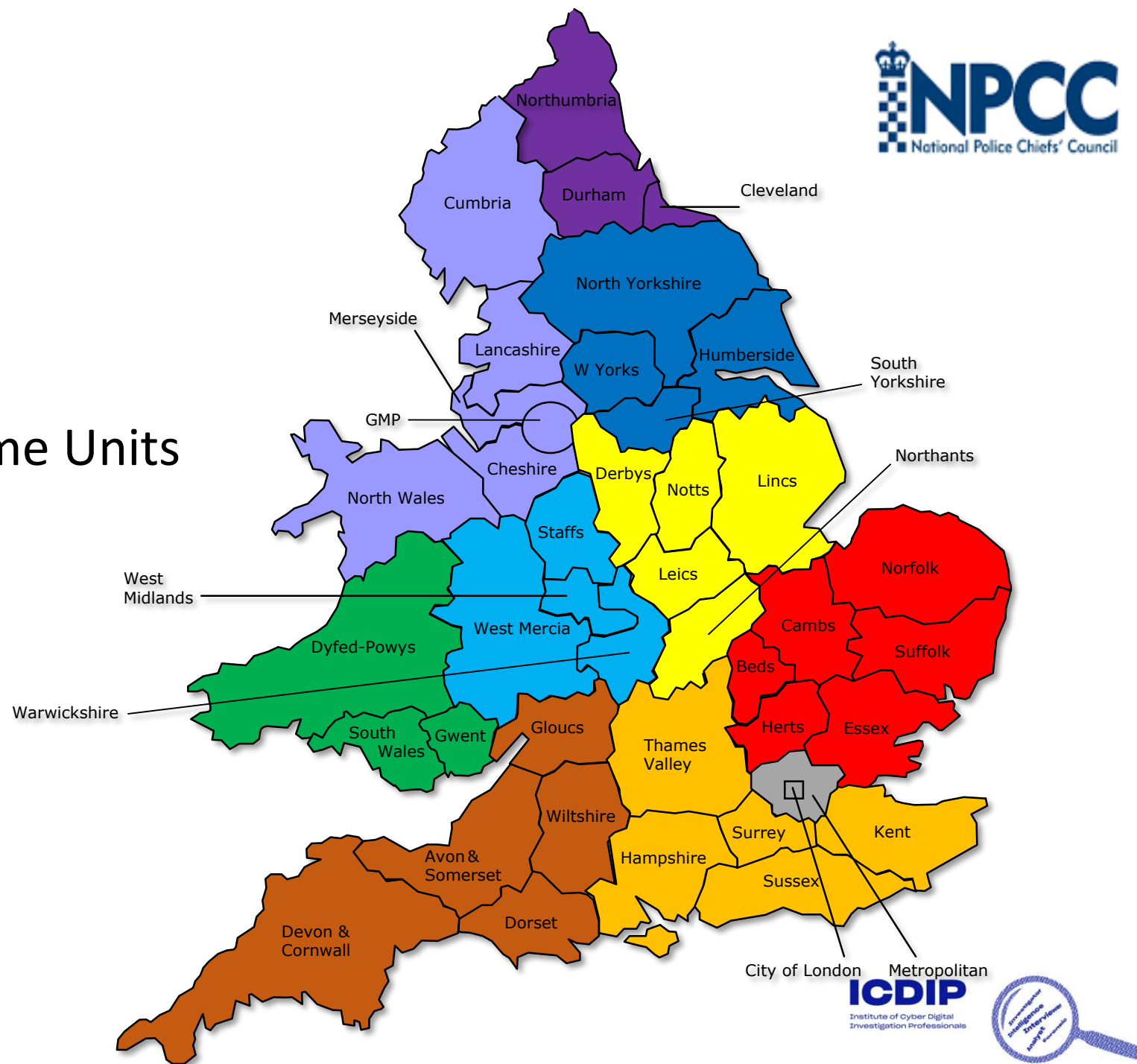
77% having
completed the
professionalisation
process they are
less likely to
consider leaving
Law Enforcement

Benefits:

- Evidence that is “admitted” not challenged in court
- Influencing decision to stay in LE
- Professionalising investigation (and aligned to cyber security profession)
- Interoperability- increased resilience and skill sharing
- Accredited & quality assured training to maintain CPD

Training

- 43 Local police forces
- 10 Regional Organised Crime Units
- 1 National Crime Agency



College of Policing (CoP)

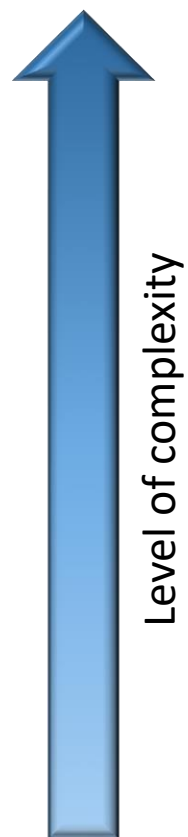
- National and International
- Professional body for everyone who works for the police service in England and Wales. (+LEAs)
- Ensure consistency across 43 forces in England and Wales
- Set standards for the police service on training, development, skills and qualification
- Focus on all policing matters not just cyber

NPCC- Team Cyber UK

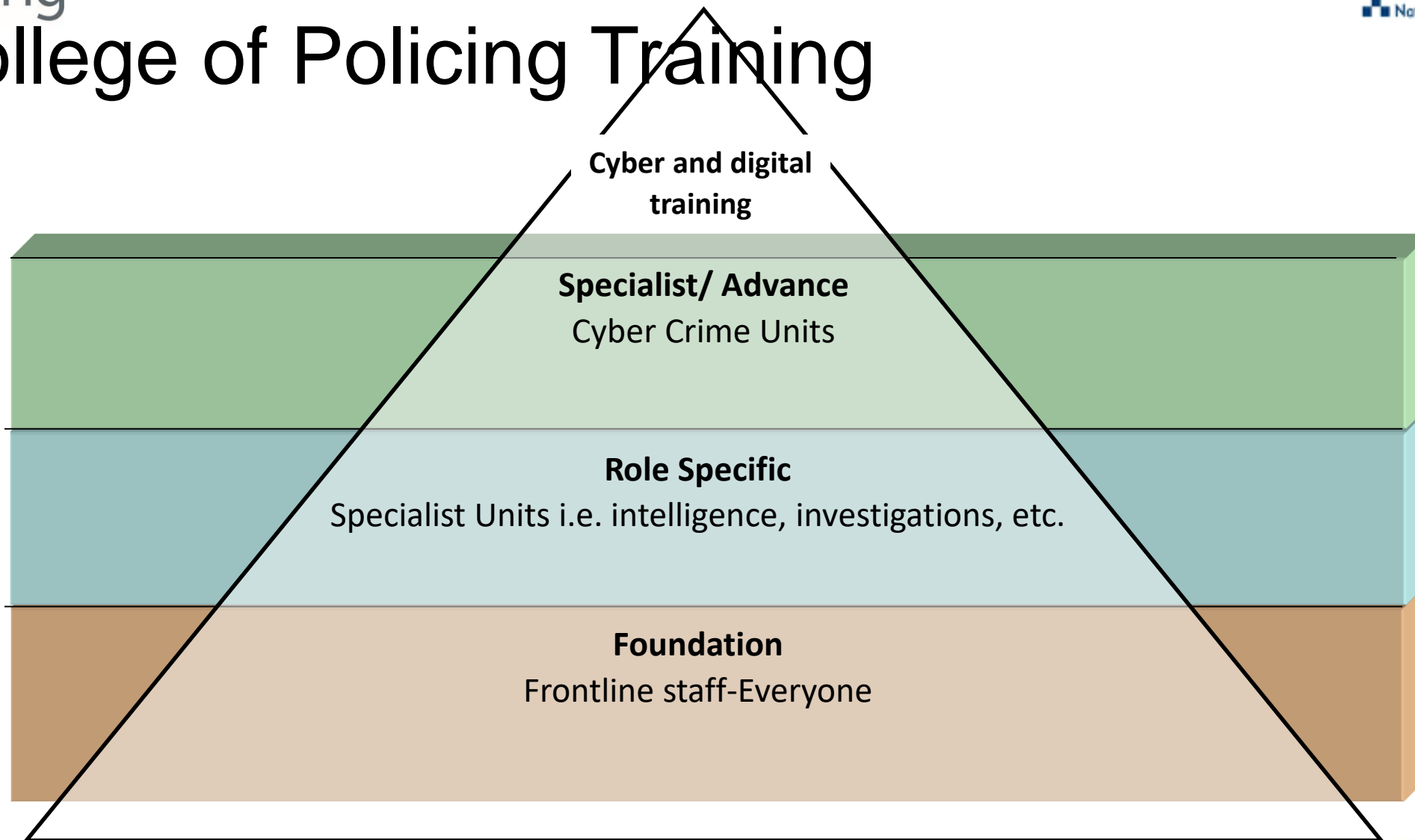
- Network-working at local, regional, National and international level. Cyber crime focused
- 4Ps: Prevent, Prepare, Protect, Pursue
- Experts in cyber crime



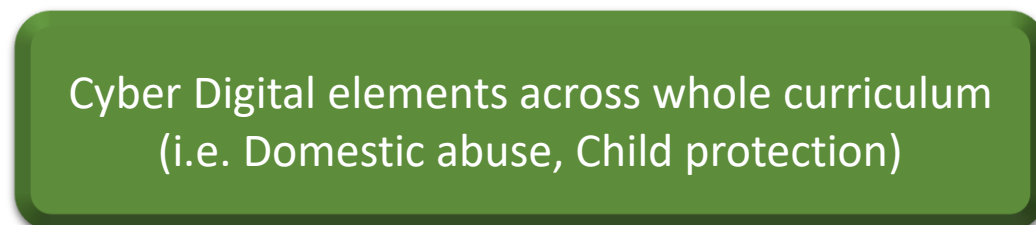
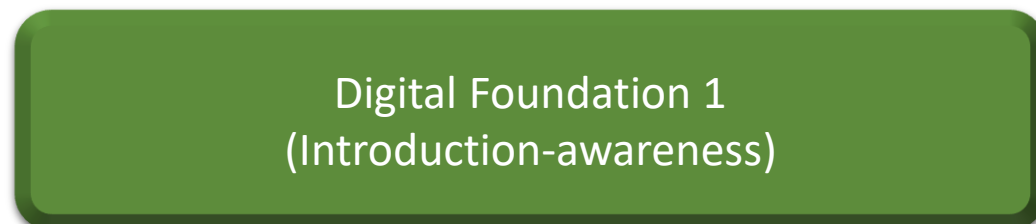
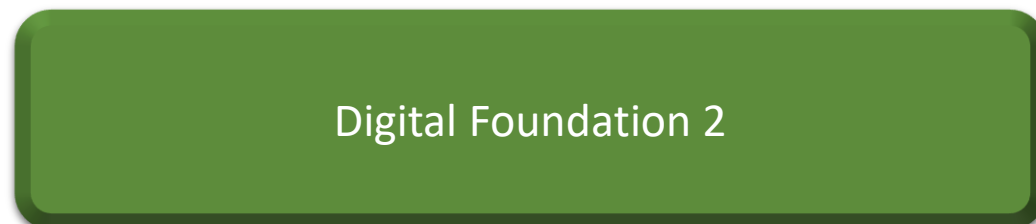
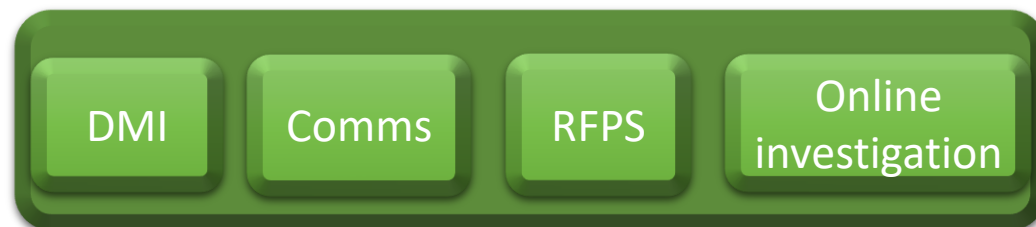
College of Policing Training



Level of complexity



College of Policing Training



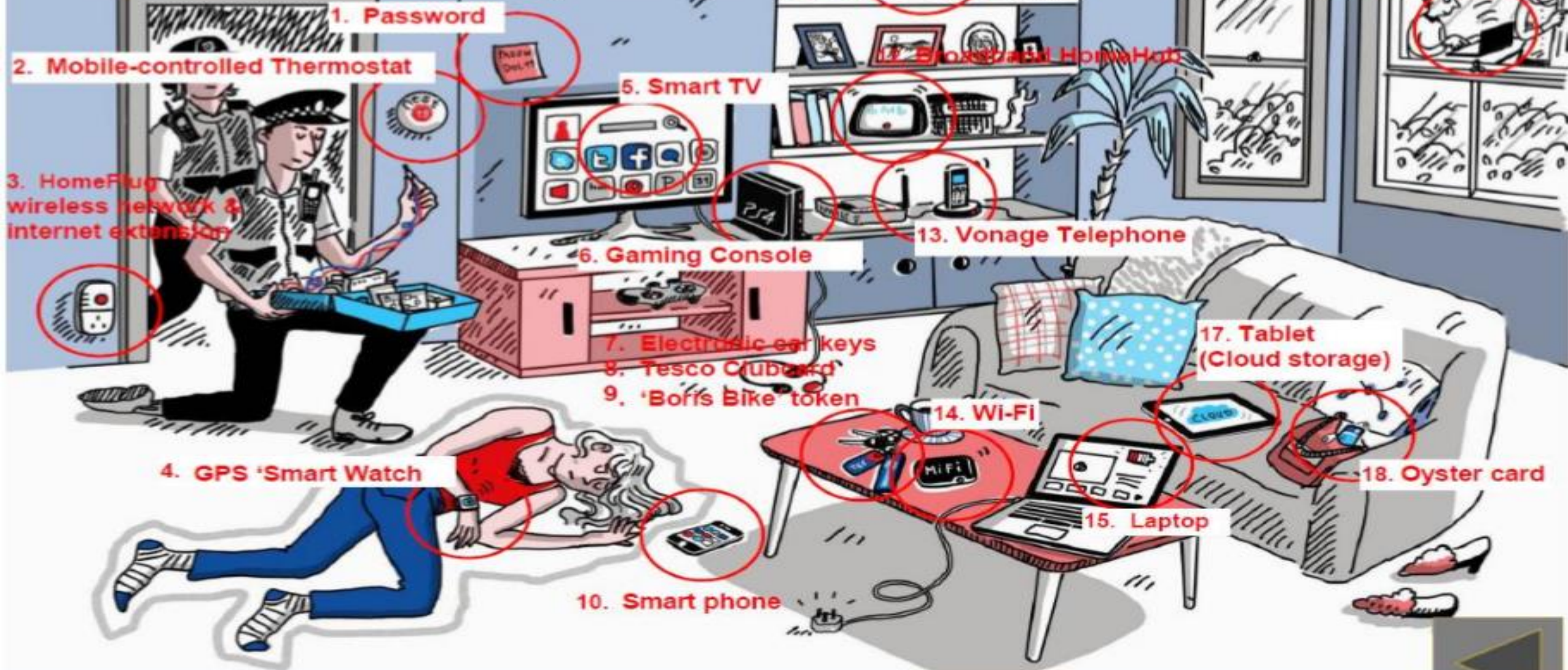
-enhanced awareness of the use/misuse of technology and how it features in the policing.
- seeks to build capabilities of a digital nature, identifying and carrying out the actions required and further ensure compliance in their actions.
- introduction to more complex internet related crime, the impact of such crime and investigative techniques (Internet, Intelligence and Investigations) for internet facilitated crimes.

-awareness of the use and misuse of technology and how it features in the policing landscape
- introduction to the criminal use of technology and devices, the involvement and use of social media and the opportunities of the Internet in relation to Intelligence and Investigations.

**THINK
DIGITAL**



THINK DIGITAL





IPC Reference	Module Title
COREE003	Professional Policing Skills
PROTA015	SCAIDP Mod 3 Investigating Child Abuse
PROTA082	Child Abuse Image Grading and Victim Identification
PROTA410	Stalking and Harassment
PRCRX003	Data Download at Ports
PRCRX007	CT Open Source Internet and Investigations (COSII)
VSTA009	Crime Scene Investigator Stage 2 (Serious and Complex Crime)
VSTA010	Crime Scene Investigator Stage 1 (Volume Crime)
VSTA112	Core Skills for Network Investigations
VSTA165	Mainstream Cyber Crime Training
VSTA168	Communications Data Profile
VSTA171	Core Skills in Mobile Phone Forensics
VSTA172	Core Skills in Data Recovery and Analysis
VSTA173	Applied NTFS Forensics
VSTA174	Researching Identifying and Tracing the Electronic Suspect (RITES)
VSTA175	Advanced Internet Forensic Traces (AIFT)
VSTA181	Advanced Network Investigator
VSTA403	Introduction to Fraud
VSTA424	Scene Preservation and Exhibits
VSTA426	Standard Search (Level 1) Premises

/SIA429*	Crime Scene Skills
/STB004	Professionalising Investigation Process PIP 2 – Supervision of Serious and Complex Investigations
/STB005	Professionalising Investigation Process PIP 2 – Management of Serious and Complex Investigations
/STB006	Fraud Investigator
/STX001	Core Skills in Communications Data
/STX002	Communications Data for Confidential Users
/STX003	Introduction to Communications Data and Cybercrime
/STX004	Investigating Digital Communications
/STX006	Lawful Intercept and Intercept Related Communications Data Induction
/STX009	Communications Data Authorising Individual
/STX020	Field Search
/STX033	Radio Frequency Propagation Survey (RFPS) Technician
/STX034	Digital Media Investigator (DMI) Initial
STX035	Radio Frequency Propagation Survey (RFPS) Practitioner
TX036	Radio Frequency Propagation Survey (RFPS) Wi-Fi and Cellular Knowledge
TX037	Digital Media Investigator (DMI) Wi-Fi
X038	Introduction to Wi-Fi
039	Vehicle Telematics Theory
166	Cyber for Investigators (MCCT2)
35	NCMLP Investigation and Intelligence
6	Communications Data Analysis
	Open Source Intelligence Research Initial
	Communications Data for Confidential Users
	Introduction to Intelligence
	Family Liaison Officer Core Knowledge
	Family Liaison Officer Crime

NPCC Cyber UK network

- January 2018 only a third of police forces had a dedicated cybercrime response
- NPCC Cybercrime Programme tasked with creating a dedicated response in every Force as part of TeamCyberUK
- Force Units coordinated by a Regional Coordinator based within the RCCU
- By April 2019 all Forces have some form of Cyber Capability working to a nationally agreed minimum standards
- Over 1000 officers and staff dedicated to Cyber Dependent Crime Operations across the 4P's





NPCC Specialist Cyber Training Framework

Specialist Cybercrime Training Framework

Introduces core concepts such as:

- types of cyber crimes and cyber attacks,
- Network security,
- operating systems
- open source intelligence,
- live forensics,
- digital forensics,
- legislation,
- principles of digital evidence.

Specialist / Advanced Training

Cyber Prevent Course

Cyber Investigator Course

Foundation in Computing, Networking and Cybercrime

Complementary Training

- Focused on incident response from a victim as well as offender perspective.
- Focused on the investigation of cyber dependant crime
- Delegates will have achieved PIP level 2

- Internet Intelligence and Investigations both overt and covert
- DMI training
- Darkweb
- Cryptocurrency





Contact:
Fiona.Paterson@college.pnn.police.uk