



College of
Policing

Leadership
Standards
Performance

Enabling Digital Investigation Workforce Capability

Sarra Fotheringham
Policing Standards Manager
Digital Policing Programme
and Data Management

Challenges of maintaining digital skills



Rapid pace of technological change outstrips current workforce development cycles, making skills quickly outdated.



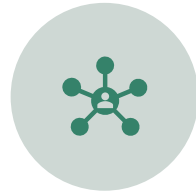
Increasing complexity of digital threats and tools requires continuous upskilling, not one-off training events.



Competing operational pressures make it difficult for officers and staff to dedicate time to sustained digital learning.



Variation in digital confidence and capability across teams creates inconsistent standards and impacts effectiveness.



Fragmented training pathways and differing national/force-level approaches limit scalability and shared learning.



High demand for specialist roles (e.g., cyber, data, digital forensics) outpaces recruitment and retention.



Need for adaptable mindsets so staff can embrace emerging technologies, automation and AI as they evolve.

Understanding the national learning programmes available to enhance digital skills



Developing National Standards



- Learning standard – Curriculum
- Guidance
- Guidelines
- Authorised Professional Practice
- Codes of Practice



Developing career pathways



Digital Investigation Foundation Course (5 days)

DIMs and their role	Tracking	Home network / Wi-Fi
Digital Strategies	Electronic monitoring	Access points
Digital Footprints	Open Source / III	Digi Dogs
Giving Evidence	Digital Crime scene	ISO standards
Modern Criminals	Types of Data	Games consoles
Working with victims	AI	Legislation
Emails	Encryption	Vehicles
Phones	Smart homes	UAVs
Call data records	House search	Cryptocurrency
Messaging apps	Cloud storage (RSED)	NFTs
Other Apps	Cloud computing	Dark web
Operating systems	Virtual computing	Interviews

 Power Point

 Digital Workbook

 Scenarios

 Discussions

 Practical

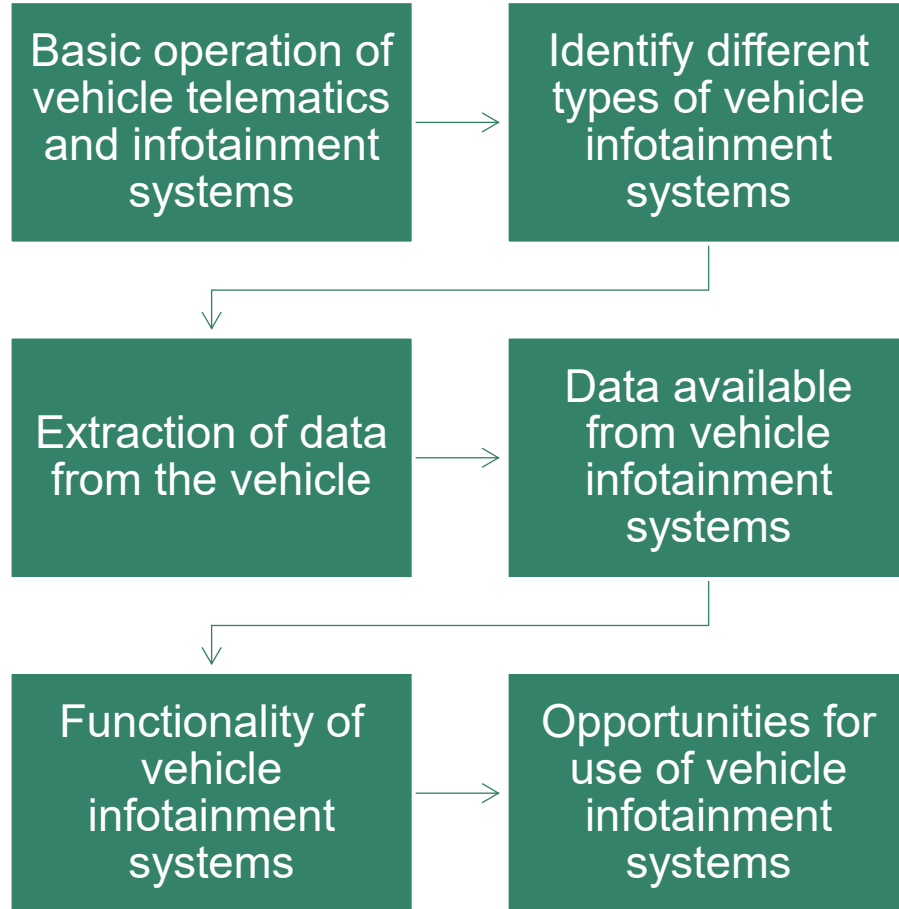
 Quizzes

Wi-Fi course (5 day)

- Understand how multiple Wi-Fi evidential sources and Wi-Fi associated technologies can assist within investigations.
- To equip learners with the skills to exploit the opportunities relating to Wi-Fi data sources and to conduct router examinations with FSR considerations.



Vehicle Systems Forensics (5 day)



Internet Intelligence and Investigation (Open source)



1. Define Internet, Intelligence and Investigations, the capability descriptors and key terms in relation to internet investigations



2. Discuss key issues and considerations in relation to tasking, legislation, record keeping and risk assessment



3. Explain and demonstrate on-line investigative techniques



4. Demonstrate how to effectively and appropriately capture evidence recovered during an on-line investigation



5. Demonstrate the ability to conduct an on-line investigation in line with an agreed III strategy



6. Discuss opportunities for researching off-line material



7. Describe what further specialist assistance is available within organisations

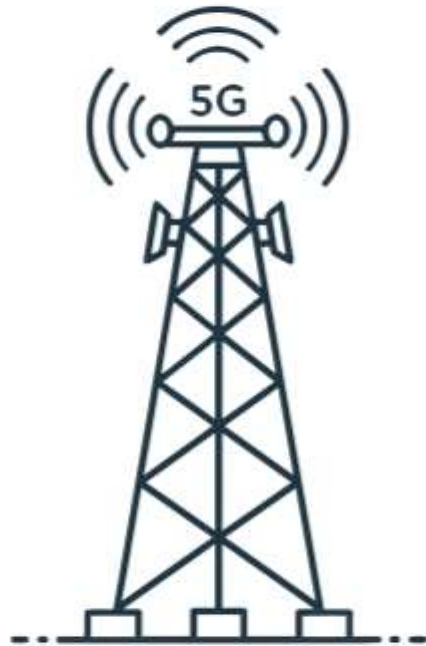
Radio Frequency Propagation Technician (10 days)

Learners who successfully complete the course will be able to:

- describe the role and responsibilities of the RFPS technician
- understand and explain network, cellular and wifi data principles
- describe the process for planning a survey
- demonstrate the practical use of tools in carrying out a survey
- identify the steps taken to create a radio frequency survey report and demonstrate preparation and presentation of results



Radio Frequency Advanced (5 days)



This course is designed to refresh the theory and practical training of the RFPS Technician course, but also to look at some aspects in more detail. It includes a practical and both the theory and practical elements will be formally assessed.

- The following topics will be covered:
- Radio theory
- 2G and 3G networks
- Cell selection processes
- Stacked cells
- 4G and GPRS sending data across cellular systems
- Survey theory – idle v dedicated
- Surveys in practice, issues you may find
- Survey planning and analysis.

Implementing a digital mindset across the whole policing eco-system

Embed	Embed digital-first thinking across operational, investigative, and support functions—treat technology as integral, not optional.
Empower	Empower the workforce with the skills, confidence and culture needed to use digital tools effectively and ethically.
Harness	Harness data as a strategic asset, enabling intelligence-led decision-making and proactive threat detection.
Accelerate	Accelerate adoption of innovative technologies such as automation, advanced analytics, and AI to enhance efficiency and effectiveness.

A unified, human-centred approach to law enforcement transformation

1

Strengthen **cross-agency collaboration** through shared platforms, **interoperable systems**, and **consistent digital standards**.

2

Prioritise **digital trust and public confidence** through secure systems, transparent use of technologies, and strong governance.

3

Modernise processes end-to-end, reducing manual burden and freeing officers and staff to focus on high-value activity. **Centre of Police Productivity and National Centre for Artificial Intelligence in Policing**

4

Create a resilient digital infrastructure capable of supporting future threats, emerging crime types, and evolving public expectations.

Contact us:

Jimmy.Battle@college.police.uk

David.Jervis@college.police.uk

Andy.McLean@college.police.uk