Liverpool John Moores University

Title:	Evidence-Based Policing 1
Status:	Definitive
Code:	**4205PSDA** (125634)
Version Start Date:	01-08-2021
Owning School/Faculty:	Justice Studies
Teaching School/Faculty:	Justice Studies

Team	Leader
Ann Stevens	Y

Academic Level:	FHEQ4	**Credit Value:**	20	**Total Delivered Hours:**	81.5
Total Learning Hours:	200	**Private Study:**	118.5		

Delivery Options
Course typically offered: S1, S2, Sum, NS2 (S2 for Jan)

Component	Contact Hours
Lecture	48
Seminar	22
Workshop	10

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Essay	Essay	2000 word essay	50	
Exam	Exam	1.5hr unseen examination, incorporating MC questions	50	1.5

Aims

To provide the students with an appreciation of the concept of evidence-based policing. Discussing a range of key concepts relating to criminology, exploring the relationship between community engagement, crime prevention, and the local force strategy for developing an effective digital policing capability.

Students will be able to identity the importance of information and intelligence to all areas of policing. Recognising the impact data protection regulations, have upon professional policing, whilst identifying practical issues pertaining to the collection, retention and sharing of information and intelligence.

Learning Outcomes

After completing the module the student should be able to:

1 Explain the professional concept of evidence-based policing, identifying potential sources of evidence that can be used as part of the evidenced based policing approach. Consider the relevance of different approaches, demonstrating evidenced based practice utilising appropriate problem solving techniques. (Please note that this is an over-arching learning objective which covers the College of Policing objectives 1 and 2)

2 Explore the relationship between community engagement and crime prevention, linking sources to specific crime problems by examining a range of key concepts relating to criminology, exploring the relationship between offending and victimisation. (Please note that this is an over-arching learning objective which covers the College of Policing objectives 3 and 4)

3 Consider the role of the police constable in dealing with internet facilitated crime, the key terms and behaviours used to initiate internet crime, and the legislation, policies and procedures available to prevent such crimes, that also deal with victims and perpetrators.

4 Identify the procedures of storage and retention of evidence.

5 Evaluate digital policing capability in today's modern society, reviewing the use of such technology within their investigations, to combat internet related crimes and protect those who may be vulnerable from such crimes. Reflect on, and debate the local force strategy for developing an effective digital policing capability. (Please note that this is an over-arching learning objective which covers the College of Policing objectives 7 and 8)

6 Outline the importance of information and intelligence to all areas of policing discussing the social and legal issues around how it might be acquired and who it can be shared with. Demonstrate an awareness of data protection legislation including the implications and penalties when the correct data management procedures are not followed. (Please note that this is an over-arching learning objective which covers the College of Policing objectives 9 and 10)

Learning Outcomes of Assessments

The assessment item list is assessed via the learning outcomes listed:

2000 word Essay	1	2	3	4	5
Unseen Exam	2	3	4	5	6

Outline Syllabus

Evidenced-based Policing and Problem solving.
Criminology and Crime Prevention.
Digital Policing.

Information and Intelligence.

Learning Activities

Lectures, Seminars, Workshops, Directed learning.

Notes

Lectures and other activities will provide the students with information, which they will then be able to apply practically, within the tasks and experiences incorporated into the workshops. Discussions and activities such as the importance of information and intelligence to all areas of policing. Students will also identify the impact of data protection regulations have upon professional policing.

Curriculum Related Objectives
1 Explain the professional concept of evidence-based policing, identifying potential sources of evidence that can be used as part of the evidenced based policing approach. Consider the relevance of different approaches.
2 Examine evidenced-based policing in practice, demonstrating the principles of problem-solving techniques.
3 Explore the relationship between community engagement and crime prevention, linking sources to specific crime problems.
4 Examine a range of key concepts relating to criminology, exploring the relationship between offending and victimisation.
5 Consider the role of the police constable in dealing with internet facilitated crime, the key terms and behaviours used to initiate internet crime, and the legislation, policies and procedures available to prevent such crimes, that also deal with victims and perpetrators.
6 Identify the procedures of storage and retention of evidence.
7 Debate the local force strategy for developing an effective digital policing capability.
8 Evaluate digital policing capability in today's modern society, reviewing the use of such technology within their investigations, to combat internet related crimes and protect those who may be vulnerable from such crimes.
9 Outline the importance of information and intelligence to all areas of policing, discussing the social and legal issues around how it might be acquired and who it can be shared with.
10 Identify the data protection regulations and their impact upon professional policing, and the implications and penalties that can arise when data management protocols are not adhered to.

Indicative Content:
Evidence Based Policing
1 Explain the professional concept of evidence-based policing
1.1 Definition of evidence-based policing (EBP): • Definitions of evidence-based policing • College of Policing definition - ATLAS approach • Sherman definition • Realist perspectives

1.2 The rationale for evidence-based policing: • Cognitive biases and heuristics e.g. Daniel Kahneman • Behavioural insights e.g. the concept of 'nudge' • High-risk, highharm, high-cost issues • 'Scared straight' and 'backfire'
1.3 Importance of differentiating between types of evidence to identify best practice: • Types of evidence: - Research evidence (types and standards of research) - Professional expertise - Information and intelligence - Lessons learned from success and failure • How evidence should be used to inform decisions: - Systematic analysis - Identification of best practice
1.4 Case studies exploring the impact of evidence-based policing in different areas of policing

2 Evaluate the potential professional applications of an evidence-based policing approach
2.1 Professional contexts in which an evidence-based policing approach is appropriate: • Organisational • Community
2.2 Policing-related activities where an evidence-based policing approach is beneficial: • Tackling crime and disorder • Managing offenders • Criminal justice • Engaging the public • Learning and development • Improving work practices/processes • Introducing new technology

3 Identify potential sources of evidence that can be used as part of an evidencebased policing approach
3.1 Sources of research and evidence (and support) for evidence-based policing: • College of Policing (What Works Centre, POLKA, National Police library, global policing database) • Other police forces • HMICFRS • Campbell Collaboration • Academic sources and journals • Government (ONS, Home Office) • Alliance for Useful Evidence/NESTA • Society of Evidence-Based Policing • Center for EvidenceBased Crime Policy (US) • Center for Problem-Oriented Policing (US)

4 Apply evidence-based policing in practice
4.1 Development of police standards (e.g. Authorised Professional Practice (APP))
4.2 Development of national/local policy (e.g. funding, deployment)
4.3 How to use evidence in practice: • Professional judgement • The reflective practitioner
4.4 How to question and challenge using evidence
4.5 Ethical concerns with regards to evidence and how these concerns can be addressed

Problem Solving
5 Explain the principles of problem-solving techniques
1.1 Herman Goldstein's model of problem-oriented policing (POP)
1.2 Models used in problem solving and crime prevention: • SARA (Scanning, Analysis, Response & Assessment) model • Problem Analysis Triangle • Routine Activity Theory • Rational Choice Theory
1.3 Principles of problem-solving and crime prevention: • Principles of crime prevention • Primary/secondary/tertiary prevention • Situational crime prevention • Early intervention and action

1.4 Evidence-based policing examples exploring the impact of evidence-based policing in different areas of policing
1.5 Partnership working and co-production in problem-solving
1.6 Role of the public in community problem-solving (e.g. problem identification and definition, taking action and assessing effectiveness)
1.7 Traditional versus non-traditional responses to problems
1.8 Outcomes of similar approaches in other comparable forces/organisations

6 Engage in effective problem solving
2.1 The importance of defining a problem: • Context of the problem • Particular features of the problem (nature, extent and causes) • Multiple sources of data/information to help define and understand the problem • Overcoming barriers to sharing partner data
2.2 Enablers to effective problem-solving
2.3 Barriers to effective problem-solving
2.4 Tools for effective problem-solving: • Problem Analysis Triangle • Routine Activity Theory • Signal Crimes • Techniques of Crime Prevention • 55 Steps to becoming a Problem-Solving Analyst
2.5 Impact of short-term targets versus long-term problem-solving e.g. priority crime types
Criminology and Crime Prevention

7 Examine a range of key concepts relating to criminology
1.1 An introduction to criminology and sociology
1.2 Crime, victimisation and harm: • Definition • Measurement • Trends and patterns • Causes

8 Explore nature of, and relationship between, offending and victimisation in light of theoretical approaches to criminology.
2.1 Offenders and offending: • Risk and vulnerability • Criminal careers and desistance from crime • Environmental criminology
2.2 Victims and victimology: • Risk and vulnerability • Repeat victimisation
2.3 Relationship between offenders and victims: • Overlap • Restorative justice

9 Examine the relationship between community engagement and crime prevention.
3.1 Definition of 'procedural justice' (See also under 'Understanding the Police Constable Role' and 'Community Policing') 3.2 Application of procedural justice

Digital Policing
10 Understand the prevalence of technology and devices in modern society and their effect on policing
1.1 Changing world of devices and device capabilities: • Wearables (e.g. fitbits, apple watches etc.) • GPS, satnav, drones • Vehicle data (telematics, infotainment etc.) • Internet of things (connected home) • Games consoles (e-readers, other mobile devices) • Routers, Wi-Fi, VPN and communications data • Data storage, including Cloud, removable drives, memory sticks and volatile data
1.2 Common IT terminology associated with devices: • Internet addresses (e.g. IP

addresses, MAC addresses, mobile internet etc.) • Email • Social networking (e.g. social media, instant messaging)• Mobile apps • Source code • Cryptocurrency • Dark web, deep web
1.3 Supporting technology and how these support device functionality • Social networks • Apps and encrypted communications
1.4 Influences in policing, of technology and devices: • First point of contact, social media etc. • Digital witnesses (Echo, Google home etc.), CCTV, digital devices etc . • Investigative opportunities (CPIA 1996, investigative mindset) • Community engagement

11 Identify and manage the personal and organisational risks associated with using personal devices and being a member of law enforcement
2.1 How to manage the security risk to self, and family: • Keeping private life separate from work life and work identity • Risk of being traced through technology, location service data etc. • Social media association
2.2 What is meant by the term 'digital hygiene': • Impacts of using personal devices for police business (e.g. automatic connection to networks, taking photographs etc.) • Seizure of the personal device for evidence and subsequent disclosure at court (e.g. crime scene photographs) • Risk of disclosure of personal data in court (if the device is seized) • Risk of leaking information about live police operations • Tracking and scanning devices
2.3 Key legislation applicable to ensure compliance and mitigate organisational risk when dealing with devices in a policing context: • Computer Misuse Act 1990 • Wireless Telegraphy Act 2006 • Criminal Justice and Police Act 2001 • Investigatory Powers Act 2016 • Regulation of Investigatory Powers Act 2000 • Police and Criminal Evidence Act 1984 • Criminal Procedure and Investigations Act 1996 • ACPO Principles of Computer Based Digital Evidence 2012 • Data Protection Act 2018/General Data Protection Regulation 2018

12 Describe the ways in which technology may be used in everyday policing
3.1 How technology may be used in a policing context: • Community engagement • Managing incidents (instant messaging, public appeals for information etc.) • Enhancing a criminal investigation (device location, attribution etc.) • Enhancing communications
3.2 Considerations regarding the use of technology within policing: • Legal restrictions on investigatory use of technology • Digital footprint, personal and work devices • Professional standards • Disclosure considerations

13 Examine types of internet-facilitated crimes, and individuals who may be especially vulnerable
4.1 Common internet-facilitated crimes: • Hate crime • Extortion (e.g. sexting/revenge porn etc.) • Abuse, bullying, stalking and threats or harassment • Online fraud/cybercrime • Child sexual exploitation • Radicalisation • Financial crime (See also under 'Vulnerability and Risk')
4.2 Individuals who may be more vulnerable to internet-facilitated crimes e.g.

children, elderly, vulnerable adults

14 Explain the role of the police in providing crime prevention advice for crimes with a digital element
5.1 Immediate actions that can be taken to reduce the risk of, and harm caused by internet-facilitated crimes, including: • Password protection • Social media 'blocking' options • Reviewing security and privacy settings • Control of personal data • Public Wi-Fi security considerations • Data back-up • Anti-virus software • Email considerations (phishing etc)
5.2 Support agencies that can provide crime prevention advice for digital devices e. g. Get Safe Online, Child Exploitation and Crime Prevention (CEOP), National Cybercrime Security Centre (NCSC) etc.
5.3 Local crime prevention strategies (see also under 'Community Policing'

15 Provide an appropriate initial police response to a report of an incident involving digital devices
6.1 How to recognise that reported incident involves a digital element
6.2 Identification of digital devices that may be involved in an investigation
6.3 Good practice for protection of the crime scene , including: • Digital hygiene • WiFi connectivity • Indicators of digital devices when searching premises, vehicles and persons • Digital witnesses • Securing devices, ensuring evidence is not corrupted, lost or deleted • Interactions e.g. interactions with any device, including vehicles, can affect output (See also under 'Response Policing')
6.4 Forensic considerations for crime scenes involving digital devices, including: • What is and is not possible • Forensic strategy (including proportionality, objective setting etc.) • Legislation and policy regarding search and seizure of devices • ACPO Principles of Computer Based Digital Evidence 2012
6.5 Specialist roles and assistance/guidance available for investigations involving digital devices: • In-force experts/Single Points of Contact (SPOCs) • Internet, intelligence and investigations specialists • Digital Media Investigators • Cyber Crime Units • Crime Prevention Units • Authorised Professional Practice
6.6 Good practice, and use of the Victims' Code when working with victims of internet-facilitated crimes, including: • Provide support to victims • Initial actions/advice • When it is appropriate to refer to partner agencies e.g. Action Fraud • Vulnerable people • Crime prevention advice • On-going support

16 Apply appropriate processes for assessing and seizing digital evidence as part of a policing response
7.1 Digital evidence opportunities (internet, intelligence and investigations), including: • Advice on obtaining screenshots • Awareness of archiving tools • Capturing online content • Tracking stolen devices • Internet telephony and its use • Email header preservation
7.2 Evidential processes when using data or devices as part of a case file, including: • How to use data from a device as evidence • Where data from a device fits, in the evidential chain • How to prepare digital evidence as part of a case file following an investigation • Compliance with relevant legislation e.g. CPIA 1996

Information and Intelligence

21 Explain the importance of information and intelligence to all areas of policing
1.1 Information versus intelligence
1.2 The National Intelligence Model (NIM)
1.3 Intelligence roles: • National intelligence • Local intelligence • Intelligence roles within other intelligence organisations 1.4 How information and intelligence can be used in key areas of policing: • Community policing • Response policing • Policing the roads • Investigation • Counter terrorism • Public protection • Vulnerability and risk • Major policing operations
1.5 Potential impact on public perceptions of policing caused by both effective/ineffective use of information and intelligence

22 Understand and operate within relevant legislation/guidance underpinning information and intelligence in policing
2.1 Relevant legislation, including: • Data Protection Act 2018/General Data Protection Regulation 2018 • Human Rights Act 1998 • Protection of Freedoms Act 2012 • Freedom of Information Act 2000 • Regulation of Investigatory Powers Act 2000 • Investigatory Powers Act 2016
2.2 Relevant guidance, including: • Managing Information (formerly Management of Police Information (MOPI)) • APP Information Management • Government Security Classifications (GSC) • Information Sharing Agreements (ISA)

23 Demonstrate an understanding of practical issues pertaining to the collection, retention and sharing of information and intelligence
3.1 The Intelligence Cycle: • Collection • Development • Dissemination
3.2 Relationship between the National Intelligence Model (NIM) and the Intelligence Cycle
3.3 Use of information and intelligence within the National Decision Model (NDM)
3.4 Sources of information and intelligence, including: • Open/closed sources • Police National Computer (PNC) • Police National Database (PND) • Policing registers • Other forces/agencies • Covert Human Intelligence Sources (CHIS) • Social media • Community intelligence
3.5 Systems employed to 'grade' information into intelligence
3.6 Uses (and challenges) of technology in information and intelligence management: • 'Golden Nominal' concept
3.7 Definition of the terms 'dissemination' and 'sharing' in relation to the managementof police information
3.8 Reasons why there is a need to share information within the police service and with other organisations
3.9 Potential positive and negative impact on policing outcomes of information and intelligence sharing
3.10 Principles of sharing police information
3.11 The different types of sharing: • Statutory obligation • Statutory Power • Common Law (Policing Purpose)
3.12 Appropriate, effective and legal sharing of information
3.13 How Information Sharing Agreements (ISAs) work

3.14 Role of the Information Commissioner's Office (ICO)
3.15 Potential consequences of sending too much information versus too little to partner agencies
3.16 Instances when sharing information outside of the ISA may be acceptable
3.17 Impacts of information misuse
3.18 Freedom of Information and subject access requests

24 Understand how information and intelligence held by other agencies can help police operations
4.1 The information that is held on individuals by other agencies
4.2 Considerations for partnership working e.g. data protection, data sharing/quality, privacy, risk management
4.3 How the sharing of information can assist in single or multi-agency operations
4.4 How to provide feedback on information and intelligence post-operation

25 Explain data protection regulations and their impact on professional policing
5.1 The key roles in information handling, including the Information Asset Owner (IAO)
5.2 Data protection regulations associated with storage, processing, use and sharingof policing data
5.3 Impact of holding incorrect, inaccurate or out of date information on an individual
5.4 Implications of data protection regulations on the use of information and intelligence in policing operations
5.5 Use of Privacy Impact Assessments with any held data
5.6 Retention periods for information
5.7 Data quality
5.8 Concept of risk mitigation

26 Examine the issues that can arise when data management protocols are not adhered to
6.1 Impacts on the police service and the reputation of policing when data management errors occur
6.2 Potential cost to the organisation and individuals when data breaches occur
6.3 Initial actions for dealing with data breaches and the roles of key stakeholders

27 Review the rights of the individual in respect of information held about them
7.1 Rights of the individual and exceptions, including: • Protection of Freedoms Act 2012 • Human Rights Act 1998

28 Understand the considerations associated with managing information and intelligence regarding vulnerable people
8.1 How data about vulnerable people is obtained and handled within the police service
8.2 The role of the intelligence manager in ensuring the intelligence is correctly risk assessed and appropriately actioned 8.3 Practices for ensuring that data is stored in the correct manner
8.4 How to ensure information is shared appropriately between the police and a range of other agencies
8.5 How to 'weed out' old and incorrect information and intelligence