Module Proforma

Approved, 2022.02

Summary Information

Module Code	5304PS
Formal Module Title	Criminal Law, Practice and Procedure 2
Owning School	Justice Studies
Career	Undergraduate
Credits	20
Academic level	FHEQ Level 5
Grading Schema	40

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings
Keith Silika	Yes	N/A

Module Team Member

Contact Name	Applies to all offerings	Offerings

Partner Module Team

Contact Name	Applies to all offerings	Offerings

Teaching Responsibility

LJMU Schools involved in Delivery
Justice Studies

Learning Methods

Learning Method Type	Hours

Lecture	22
Online	11
Workshop	22

Module Offering(s)

Offering Code	Location	Start Month	Duration
JAN-MTP	MTP	January	12 Weeks

Aims and Outcomes

Aims	To provide the students with the knowledge and understanding of legislation and police powers in relation to terrorism and counterterrorism measuresEnable students to apply such knowledge to a range of specified circumstances and incidents.

Learning Outcomes

After completing the module the student should be able to:

Code	Description
MLO1	Demonstrate knowledge and understanding of the various pieces of the legislation and the resulting police powers relating to terrorism.
MLO2	Demonstrate knowledge and understanding of the legislation and the resulting police powers relating to digitally dependent and digitally enabled crime.
MLO3	Demonstrate understanding of the wider issues relating to digitally dependent and digitally enabled crime.
MLO4	Demonstrate understanding of the wider issues impacting upon terrorism and the police responses.

Module Content

Outline Syllabus
Digital technology and implications for policing Cybercrime and cyber enabled crime UK Counter-terrorism strategy. UK National Security Strategy.

Module Overview
This module will provide you with the knowledge and understanding of legislation and police powers in relation to terrorism and counterterrorism measures. It will enable you to apply such knowledge to a range of specified circumstances and incidents.

Additional Information

Lectures and other activities will provide the students with information. Students will then apply the knowledge acquired to a range of scenarios and situations incorporated into the workshops. Discussions and activities, in the seminars will explore the subject in greater depth and broader context. National Policing Curriculum Indicative Content Digital Policing 1.1 Changing world of devices and device capabilities: • Wearables (e.g. Fitbit, 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 of technology and devices in a policing context • 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 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 3.1 How digital technology may be used to assist with: • Community engagement • Managing incidents (instant messaging, public appeals for information etc.) • Enhancing a criminal investigation (device location, attribution etc.) • Enhancing communications 3.2 Considerations in the use of technology within policing: • Legal restrictions on investigatory use of technology • Digital footprint, personal and work devices • Professional standards • Disclosure considerations 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 4.2 Individuals who may be more vulnerable to internet-facilitated crimes e.g. children, elderly, vulnerable adults 5.1 How criminals engage in complex internet-dependent crimes and the impact of such criminality: • Hacking • Malware • Phishing • Denial of service • Browser hi-jacking • Ransomware • Data manipulation • Cryptocurrency and cryptolocker offences 5.2 Impact of complex digital-related crimes on individuals and businesses Counter Terrorism 1.1 Radicalisation 1.2 Extremism, including domestic extremism 1.3 Interventions 1.4 Terrorism-related offences 1.5 CONTEST strategy: Pursue, Prevent, Protect and Prepare 2.1 National Counter Terrorism Policing HQ (NCTPHQ)

All assessed components on this module must be successfully passed for credit to be released.

Assessments

Assignment Category	Assessment Name	Weight	Exam/Test Length (hours)	Learning Outcome Mapping
Centralised Exam	Exam MC and Seen	100	2	MLO4, MLO2, MLO1, MLO3