Module Specification

Digital Policing

Version: 2024-25, v2.0, 18 May 2022

Contents

Part 1: Information

Module title: Digital Policing

Module code: UZSYG8-15-3

Level: Level 6

For implementation from: 2024-25

UWE credit rating: 15

ECTS credit rating: 7.5

Faculty: Faculty of Health & Applied Sciences

Department: HAS Dept of Social Sciences

Partner institutions: None

Delivery locations: Frenchay Campus

Field: Sociology and Criminology

Module type: Standard

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: This module provides an insight into the changing world of technology as relevant to the policing context. Learners will examine a range of internet and digitally facilitated crimes and the different ways people can be vulnerable to these alongside thinking about the ways in which technology can aid policing.

Features: Not applicable

Educational aims: This module aims to provide learners with a broad overview and understanding of the prevalence of technology and devices in modern society and their effect on policing through the exploration of the changing world of devices and device capabilities. This will include wearables, GPS, telematics, smart speakers, games consoles, Wi-Fi routers and any device capable of connecting to the internet and cloud-based storage networks. Learners will explore common IT terminology associated with digital devices such as internet addresses, email, social networks and mobile phone apps, source code, cryptocurrency, and the dark and deep web. The module identifies supporting technology and explains how these support device's functionality as well as analysing influences of technology and devices in a policing investigative context.

The module highlights the personal and organisational risks associated with using personal devices and being a member of law enforcement and details how to manage the security risk to self and family, and debates the importance of keeping their private life separate from their work life and work identity, and introduces measures to mitigate the risk of being traced through technology by means of location-based services and social media association.

'Digital hygiene' is a term used to describe a person's presence (footprint) on the internet and how secure their accounts may or may not be. This module provides a valuable insight on how to review and scrutinise your own digital footprint and describes the level detail required within online crime prevention action plans which could be provided to members of the public. The module scrutinises the impact of using personal devices for police business (such as automatic connection to wireless networks or crime scene photographs) and the potential for personal devices being seized as evidence, and subsequent disclosure at court in addition to highlighting the risk and impact of disclosure of personal data in court (if the device is seized) and the risk of leaking information about live operations. Key legislation applicable to ensuring compliance and the mitigation of organisational risk when dealing with devices in a policing context are prominently referenced to within the module.

Technology may be used in everyday policing from the gathering of information from victims and witnesses, including further lines of enquiry, to managing incidents,

enhancing criminal investigations, and enhancing communications. The module will explain how data is retained in apps on devices and be able to summarise the legal restrictions on investigatory use of technology, professional standards, disclosure considerations and considerations associated with unlawful research/examination of a device, including assuming a fake persona.

The module examines the types of internet-facilitated crimes, and individuals who may be especially vulnerable, and provides opportunities for learners to formulate strategies which protect individuals who may be more vulnerable to internet-facilitated crimes, particularly children, the elderly, and vulnerable adults. By first describing the complex types of digital-facilitated crimes and their impact on individuals and businesses, the module develops awareness of additional sources of intelligence that can be obtained during a complex investigation and explains the roles of specialists in retrieving information/intelligence or evidence from devices.

Outline syllabus: Cop Curriculum:

Digital Policing:

1 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 a policing context, 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 mind-set)
• Community engagement

2 Understand 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:

• Police and Criminal Evidence Act 1984
• Computer Misuse Act 1990
• Criminal Procedure and Investigations Act 1996
• Regulation of Investigatory Powers Act 2000
• Criminal Justice and Police Act 2001
• Wireless Telegraphy Act 2006
• ACPO Good Practice Guide for Digital Evidence 2012

• Investigatory Powers Act 2016
• Data Protection Act 2018
• General Data Protection Regulation (EU) 2016/679 (GDPR)

3 Describe the ways in which technology may be used in everyday policing

3.1 How digital technology may be used to assist with:

• Community engagement
• Data retained in apps on devices e.g. locations
• Gathering information, including further lines of enquiry (victims, suspects and witnesses)
• 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

3.3 Considerations associated with unlawful research/examination of a device, including assuming a fake persona

5 Describe the specialist support available for investigations involving digital devices

5.1 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 Describe complex types of digital- dependent crimes and their impact

6.1 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

6.2 Impact of complex digital-related crimes on individuals and businesses

Police Investigations:

6 Understand the additional sources of intelligence that can be obtained during a complex investigation

6.1 Role of specialists in retrieving information/intelligence or evidence or material from devices

Part 3: Teaching and learning methods

Teaching and learning methods: The module will employ a combination of lectures, seminars, and workshops. Our pedagogy is interactive, discussion-based, and student-facing. Students are an active part of the learning process, and will be asked to contribute ideas, questions, and critical standpoints. The learning environment is designed to promote peer-to-peer support and exchange.

While teaching and learning will be predominantly classroom based, appropriate use will be made of online resources and learning environments.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Discuss the changing world of digital devices, the range of devices available, their capabilities and identify how to manage security risk to oneself and others including the practice of 'digital hygiene'.

MO2 Examine key legislation applicable to digital investigations to ensure compliance and mitigate organisational risk when dealing with digital devices in a policing context.

MO3 Critically evaluate the ways in which technology may be used in everyday policing.

MO4 Compare and contrast the types of internet-facilitated crimes and the individuals who may be especially vulnerable.

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 112.5 hours

Lectorials = 37.5 hours

Total = 150

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://rl.talis.com/3/uwe/lists/62EC1889-5B90-8FEC-7EC2-709D2F956D0A.html?draft=1&lang=en-GB&login=1

Part 4: Assessment

Assessment strategy: Summative assessment will be divided over two tasks, a group task, and an individual task.

Component A is a 1000-word Group Wiki / Blog on Blackboard.

Component B is a 2000-word critical analysis on a Digital policing Topic.

The assessment requires learners to develop a blog about an aspect of digital Policing and secondly an individual task which requires the critical evaluation of a particular digital policing topic.

The two tasks work together to ensure learners have an appropriately broad and

deep understanding of the relevant subject matter but can demonstrate an analytical consideration of digital policing. This is important given the ongoing innovation of criminal activity and the policing of it within the digital domain.

Formative assessment of learning will be provided during scheduled teaching activities though quizzes, taking part in discussions, debates and questions and answers during taught sessions. Additional formative support will be provided in study skills workshops on research, literature reviews, creation of abstracts, and referencing.

Assessment components:

Set Exercise - Component A (First Sit)
Description: 1000-word Group Wiki / Blog on Blackboard.
Weighting: 40 %
Final assessment: No
Group work: Yes
Learning outcomes tested: MO2

Written Assignment - Component B (First Sit)
Description: 2000 word critical analysis on a Digital policing Topic.
Weighting: 60 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4

Set Exercise - Component A (Resit)
Description: 1000-word Individual Wiki / Blog on Blackboard.
Weighting: 40 %
Final assessment: No
Group work: No
Learning outcomes tested: MO2

Written Assignment - Component B (Resit)

Description: 2000 word critical analysis on a Digital policing Topic.

Weighting: 60 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO1, MO2, MO3, MO4

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Professional Policing [Sep][FT][Frenchay][3yrs] BSc (Hons) 2022-23

Professional Policing [Frenchay] BSc (Hons) 2022-23