Module specification

**When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory**

| | |
|---|---|
| Module Code | POL504 |
| Module Title | Digital Policing and Counter Terrorism |
| Level | 5 |
| Credit value | 20 |
| Faculty | Social and Life Sciences |
| HECoS Code | 100484 |
| Cost Code | GACJ |

## Programmes in which module to be offered

| Programme title | Is the module core or option for this programme |
|---|---|
| BSc (Hons) Professional Policing | Core |

## Pre-requisites

None

## Breakdown of module hours

| | |
|---|---|
| Learning and teaching hours | 30 hrs |
| Placement tutor support | 0 hrs |
| Supervised learning e.g. practical classes, workshops | 0 hrs |
| Project supervision (level 6 projects and dissertation modules only) | 0 hrs |
| **Total active learning and teaching hours** | **30** hrs |
| Placement / work based learning | 0 hrs |
| Guided independent study | 170 hrs |
| **Module duration (total hours)** | 200 hrs |

| **For office use only** | |
|---|---|
| Initial approval date | January 2019 |
| With effect from date | September 2019 |
| Date and details of revision | January 2021 – updates made to CoP standards numbering and syllabus points |

| For office use only | |
|---|---|
| | January 2022 – minor changes to syllabus and standards numbering as per CoP requirements<br>July 2022 – change to LO wording, NPC mapping and syllabus content to meet CoP requirements.<br>Change to assessment strategy. |
| Version number | 4 |

## Module aims

To explore the nature of, and policing response to, Digital Policing and Counter Terrorism

## Module Learning Outcomes - at the end of this module, students will be able to:

| | |
|---|---|
| 1 | Understand the prevalence of technology and devices in modern society, their effect on policing and the personal and organisational risks associated with using them<br><br>(NPC mapping Digital policing : 1.1,2.1,3.1.4,2.1,2.2,2.3 ) |
| 2 | Examine how technology may be used in everyday Policing<br><br>(NPC mapping: Digital Policing: 3.1,3.2, 3.3; 5.1) |
| 3 | Examine common and complex types of digital-facilitated crimes , the individuals who may be especially vulnerable and the impact of such crimes on individuals, businesses and families<br><br>(NPC mapping: Digital policing: 4.1,4.2, 6.1, 6.2)<br>(NPC mapping Response policing 16.1, 16.2, 16.3, 16.4) |
| 4 | Understand key counter-terrorism terminology/concepts, the role of front line policing, and the organisational structures and inter-relationships that exist in counter-terrorism policing including their role/functions in past and present counter-terrorism operations<br><br>(NPC mapping: Counter Terrorism:1.1,1.6,1.2,1.3,1.4,1.5,2.1,2.2 ,2.3,2.4,2.5,2.6,2.7,2.8,2.9, 4.1,4.2 , 7.1, 7.2, 8.1, 8.2, 8.3, 8.4, 8.5) |
| 5 | Analyse the potential links between terrorism and other forms of criminality and the role of policing in gathering intelligence relevant to counter-terrorism policing<br><br>(NPC mapping: Counter Terrorism:,5.1,5.2,6.1) |
| 6 | Understand key legislation relevant to counter-terrorism policing<br><br>(NPC mapping: Counter Terrorism 3.1,3.2,4.1,4.2 ) |

## Assessment

Indicative Assessment Tasks:

This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.
There are 2 assessments for this module:

Academic Poster students will explore the history of two forms of digital crime (one common (10 mins)/one complex (10mins)), the impact it has, and authority under which, and how, police might respond (Duration: 30 minutes)

Case study requires students to devise a police counter-terrorism plan in the case of a prolific offender now a prison leaver who has been radicalised in custody and soon to be released (2,000 words)

Assessment guidance will be provided that directs students towards meeting the relevant learning outcomes

| Assessment number | Learning Outcomes to be met | Type of assessment | Weighting (%) |
|---|---|---|---|
| 1 | 1-3 | Presentation | 50% |
| 2 | 4-6 | Written Assignment | 50% |

## Derogations

Module cannot be condoned/compensated on BSc (Hons) Professional Policing
All elements must be passed on BSc (Hons) Professional Policing

## Learning and Teaching Strategies

The learning and teaching strategy used in the module is grounded in the University's commitment to Universal Design for Learning (UDL), the key principle of which holds that students are encouraged to participate in higher education when they are exposed to flexible ways of learning by staff that engage them in different ways using innovative and creative approaches. Accordingly the module embrace the University's Active Learning Framework (ALF) which supports accessible, flexible learning that creates a sense of belonging for students. Each module is associated, thereby, with face to face and online elements

## Indicative Syllabus Outline

**LO1: Understand the prevalence of technology and devices in modern society, their effect on policing and the personal and organisational risks associated with using them**

Changing world of devices and device capabilities:
- Wearables (e.g. Fitbits, Apple watches etc.)
- GPS, satnav, drones begining
- 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

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

Supporting technology and how these support device functionality
- Social networks
- Apps and encrypted communications

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

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

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

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 (EU 2016/679 (GDPR) 2018

**LO2: Examine how technology may be used in everyday policing**

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

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

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

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

**LO3: Examine common and complex types of digital-facilitated crimes , the individuals who may be especially vulnerable and the impact of such crimes on individuals, businesses and families**

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
- Modern slavery and human trafficking

Individuals who may be more vulnerable to digital-facilitated crimes e.g children, elderly, vulnerable adults
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

Impact of complex digital-related crimes on individuals and businesses
Definition of what is meant by the term Unmanned Aerial Vehicle (UAV) and the terms by which they may be known e.g. Drone, Remotely Piloted Aerial System (RPAS) etc.
Legislative requirements for flying drones, including weight, separation distances, operator registration, pilot qualifications etc.
The role of the Civil Aviation Authority (CAA) in relation to Unmanned Aerial Vehicles (UAVs) and associated CAA permissions and Operational Authorisations
Police powers available when responding to an incident involving drones, contained in the Air Traffic Management and Unmanned Aircraft Act 2021

**LO4: Understand key counter-terrorism terminology/concepts, the role of front line policing, and the organisational structures and inter-relationships that exist in counter-terrorism policing including their role/functions in past and present counter-terrorism operations**

Radicalisation
Extremism, including Right Wing Terrorism (RWT) and Left Anarchist or Single Issue Terrorism (LASIT), Northern Ireland Related Terrorism (NIRT) and Islamist Terrorism (IT)
Interventions
Terrorism-related offences
CONTEST strategy: Pursue, Prevent, Protect and Prepare
Terminology and threshold matrix
National Counter Terrorism Policing HQ (NCTPHQ)
National Counter Terrorism Policing Operations Centre (NCTPOC)
Counter Terrorism Command (CTC)
Counter Terrorism Unit (CTU)
Counter Terrorism Intelligence Unit (CTIU)
Special Branch
Security Service
National Counter Terrorism Security Office (NaCTSO)
Importance of partnership working, including international and European partners
Importance of recognising vulnerabilities in a counterterrorism context
Indicators of radicalisation of an individual:

- Risk factors
- Warning signs
- Individual and environmental factors
- Engagement, intent and capability

Definition of the 'insider threat'
The common causes of an 'insider threat' scenario e.g. data loss, disaffection, duress
Signs that a person could be vulnerable to an 'insider threat'
Impact on the organisation of the 'insider threat'
Methods

**LO5: Analyse the potential links between terrorism and other forms of criminality and the role of policing in gathering intelligence relevant to counter-terrorism policing**
Intelligence in counter-terrorism operations:

- Local
- Regional
- National

Importance of community intelligence in counter-terrorism operations:

- Community engagement
- Developing intelligence
- Fostering co-operation

**LO6:Understand key legislation relevant to counter-terrorism policing**
Methods of funding/enabling terrorism, including:

- Money laundering
- Fraud
- Identity theft

## Indicative Bibliography:

Please note the essential reads and other indicative reading are subject to annual review and update.

**Essential Reads**


- Taylor, R.W., Fritsch, E.J. and Liederbach, J., (2014). Digital Crime and Digital Terrorism. Prentice Hall Press.

Digital Policing.

- Bryant, R. ed., 2016. Policing digital crime. Routledge.
- College of Policing(2018) Digital Investigation and Intelligence Authorised Professional Practice https://www.app.college.police.uk/app-content/digital-investigation-and-intelligence/?s=
- Gillespie, A (2015) Cybercrime: Key Issues and Debates. London: Routledge
- Hitchcock, A., Holmes, R. and Sundorph, E., 2017. Bobbies on the net: a police workforce for the digital age.

- HMIC (2015) Real Livers, real crime: A study of digital crime and policing. London: HMIC https://www.justiceinspectorates.gov.uk/hmicfrs/?cat=digital&force=&frs=&year=&s=&type=publications
- McMurdie, C., 2016. The cybercrime landscape and our policing response. Journal of Cyber Policy, 1(1), pp.85-93.
- Richardson, L., Beadle-Brown, J., Bradshaw, J., Guest, C., Malovic, A. and Himmerich, J., 2016. "I felt that I deserved it"–experiences and implications of disability hate crime. Tizard Learning Disability Review, 21(2), pp.80-88.
- Wall,D.S. and Williams,M. (2014) Policing Cybercrime: Networked and Social media technologies and the Challenges for Policing


Police Counter Terrorism


- Hutton,G.,Mckinnon,G. and Connor,P. (2018) Blackstone's Police Manuals Volume 4: General Police Duties 2019 Chapter 4.9 Terrorism and Associated Offences. London: Blackstone
- Joyce,P. (2016) The Policing of Protest, Disorder and International Terrorism in the UK since 1945. London: Palgrave/Macmillan.
- McMurdie, C., 2016. The cybercrime landscape and our policing response. Journal of Cyber Policy, 1(1), pp.85-93.
- Murphy, K., Madon, N.S. and Cherney, A., 2017. Promoting Muslims' cooperation with police in counter-terrorism: The interaction between procedural justice, police legitimacy and law legitimacy. Policing: An International Journal, 40(3), pp.544-559.
- Staniforth, A. (2013) Blackstone's Counter-Terrorism Handbook. London: Blackstone
- Silke, A. ed., 2018. Routledge Handbook of Terrorism and Counterterrorism. Routledge.


**Other indicative reading**

Digital Policing


- Broadhurst, R, Grabosky, P, Alazab, M and Chon, S (2014) Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime. International Journal of Cyber Criminology Vol 8 Issue 1: 1-20..
- Gilmour, S., 2014. Policing crime and terrorism in cyberspace: An overview. European Review of Organised Crime, 1(1), pp.143-159
- Horsman, G., 2017. Can we continue to effectively police digital crime?. Science & Justice, 5 Jones, C., 2015. Managing extremist offenders: The TACT-ics of policing thought?. Probation Journal, 62(2), pp.172-180.7(6), pp.448-454.
- Loveday, B., 2017. Still plodding along? The police response to the changing profile of crime in England and Wales. International Journal of Police Science & Management, 19(2), pp.101-109.
- Gannoni, A., Willis, M., Taylor, E. and Lee, M., 2017. Surveillance technologies and crime control: understanding police detainees' perspectives on police body-worn video (BWV) and CCTV cameras.

- Blakemore, B., 2016. Policing cyber hate, cyber threats and cyber terrorism. Routledge.
- Blakemore, B., 2016. Extremism, Counter-terrorism and Policing. Routledge.
- Dunn, K.M., Atie, R., Kennedy, M., Ali, J.A., O'Reilly, J. and Rogerson, L., 2016. Can you use community policing for counter terrorism? Evidence from NSW, Australia. Police Practice and Research, 17(3), pp.196-211.
- Innes, M., Roberts, C. and Lowe, T., 2017. A Disruptive Influence?"Prevent-ing" Problems and Countering Violent Extremism Policy in Practice. Law & Society Review, 51(2), pp.252-281.
- Thomas, P., 2016. Youth, terrorism and education: Britain's Prevent programme. International Journal of Lifelong Education, 35(2), pp.171-187.
- Ragazzi, F., 2016. Suspect community or suspect category? The impact of counter-terrorism as 'policed multiculturalism'. Journal of Ethnic and Migration Studies, 42(5), pp.724-741.
- Silke, A. ed., 2014. Prisons, terrorism and extremism: Critical issues in management, radicalisation and reform. Routledge.


## Employability skills – the Glyndŵr Graduate

Each module and programme is designed to cover core Glyndŵr Graduate Attributes with the aim that each Graduate will leave Glyndŵr having achieved key employability skills as part of their study. The following attributes will be covered within this module either through the content or as part of the assessment. The programme is designed to cover all attributes and each module may cover different areas.

**Core Attributes**
Engaged
Enterprising
Creative
Ethical

**Key Attitudes**
Commitment
Curiosity
Resilience
Confidence
Adaptability

**Practical Skillsets**
Digital Fluency
Organisation
Leadership and Team working
Critical Thinking
Emotional Intelligence

Communication