MSc Cybercrime and Digital Investigations

Programme Specification

1. Programme title	MSc Cybercrime and Digital Investigations
2. Awarding institution	Middlesex University
3a. Teaching institution 3b. Language of study	Hendon, Middlesex University, London English
4a. Valid intake dates 4b. Mode of study 4c. Delivery method	September Full Time or Part Time ☒ On-campus/Blended ☐ Distance Education
5. Professional/Statutory/Regulatory body	N/A
6. Apprenticeship Standard	N/A
7. Final qualification(s) available	PG Dip Cybercrime and Digital Investigations PG Cert Cybercrime and Digital Investigations MSc Cybercrime and Digital Investigations
8. Year effective from	2022

9. Criteria for admission to the programme

Applicants must have a minimum of a 2:2 undergraduate honours degree in social sciences or above in an appropriate subject, or an equivalent qualification.

Applicants with other qualifications and/or substantial work experience in the field of criminology will also be considered under the Recognition of Prior Learning scheme. Past learning or experience will be mapped against existing programme modules within the programme and academic credit may be awarded towards the programme of study.

Overseas applicants should be competent in English and have achieved as a minimum IELTS. Overall, 6.5 with a minimum 6.0 in each component. We normally require Grade C GCSE or an equivalent qualification.

Applicants with a disability can enter the programme. The programme team have experience of adapting teaching provision to accommodate a range of disabilities and welcome applications from students with disabilities.

10. Aims of the programme

The programme aims to:

- Provide students with an understanding of the criminological and research context of cybercrime, contemporary debates surrounding the causes of cybercrime, digital investigations and the methods and motivations of cyber criminals.

- Equip students with an understanding of computing skills and capabilities that will help to respond to online threats to personal information as well as to organisational environments.

- Develop students theoretical and practical experience and knowledge of digital investigations and the use of investigatory software.

- Prepare students seeking a specialist role in a community or support service environment, such as victim support services, the police force, security governance, private charities and organisations, child protection, offender services, as well as corporate environments where there is a need to prevent and respond to cybercrime and issues related to online safety.

- Prepare students to carry out digital investigations and research using a range of digital methods.

11. Programme outcomes*

A. Knowledge and understanding
On completion of this programme the successful student will have knowledge and understanding of:

1. Current theoretical and enforcement debates in cybercrime and the applicability of cybercrime research to criminological theory, practice, and policy.
2. Contemporary methods in researching cybercrime.
3. Range of tools and techniques to carry out a digital investigation.
4. How technology facilitates and is used to respond to crime.

Teaching/learning methods
Students gain knowledge and understanding through:

- Attending lectures
- Participatory seminars/leminars
- Small group discussions/presentations
- Group and individual exercises
- Workshop and laboratory exercises
- Use of interactive creative online platforms
- Independent learning
- Directed reading
- Formative assessments
- Guest lectures

2

5. Legal and professional issues related to computer-related crime, digital evidence, and digital forensic investigations. 6. Challenges and opportunities presented by technologies for cyber analysts. 7. Investigative guidelines, and ethical practices and legislation.	**Assessment methods** Students' knowledge and understanding is assessed by: • Technical investigation report • Risk assessment report for a business • Essays • Contribution towards discussion boards • Project and portfolio work • Empirical research and analysis • Research outputs
B. Skills On completion of this programme the successful student will be able to: 1. Use relevant tools and techniques to carry out digital investigations. 2. Investigate, collect, and analyse and present relevant digital evidence from computing devices. 3. Advise on managing compliance in corporate environments and implementing tools and techniques for detecting, investigating, and preventing financial crime. 4. Evaluate new sources of research knowledge and information and those used in previous research. 5. Effectively develop and design a research proposal. 6. Use learning resources effectively in relation to researching cybercrime. 7. Criticise and engage in reasoned debate about relevant ethical digital investigation issues. 8. Plan and carry out an independent project, policy evaluation or work-based development project.	**Teaching/learning methods** Students learn skills through • Attending lectures • Participatory seminars/leminars • Small group discussions/presentations • Group and individual exercises • Workshop and laboratory exercises • Use of interactive creative online platforms • Independent learning • Directed reading • Formative assessments • Guest lectures **Assessment methods** Students' skills are assessed by • Technical investigation report • Risk assessment report for a business • Essays • Contribution towards discussion boards • Project and portfolio work • Empirical research and analysis • Research outputs

12. Programme structure (levels, modules, credits and progression requirements)

12. 1 Overall structure of the programme

- The programme can be studied over either one-year full time or two years part time.

- PGCert, full time students will take four 15 credit core modules in term one in the first year of study. Part-time students will normally take four 15 credit core modules in term one in the first year, or across the two years. The order in which this is done is the students choice.

- Students who successfully complete the 120 taught credits but who do not undertake a dissertation or <mark>work-based experience</mark> will be awarded a PGDip.

- In addition, the MSc students will take a 60-credit dissertation or <mark>work-based experience</mark> and successfully complete 180 credits.

Full Time Programme Structure for MSc Cybercrime and Digital Investigations		
<mark>Term One</mark> **(60 credits)**	<mark>Term Two</mark> **(60 credits)**	<mark>Term Three</mark> **(60 credits)**
15 CREDITS CST4230 Digital Forensics and Incident Management	**15 CREDITS** CST4220 Blockchain Anatomy and Analytics	
15 CREDITS CST4240 Financial Crime Risks from Emerging Technologies	**15 CREDITS** CST4250 Open-source Intelligence Techniques	
15 CREDITS CRM4615 Cybercrime and Society	**15 CREDITS** CRM4630 Text Mining and Analysis	
15 CREDITS CRM4629 Research Strategies in Social Sciences	**15 CREDITS** OPTIONAL MODULE	
	60 CREDITS CRM4617 Dissertation **OR** <mark>CRM4XXX - Work-Based Experience</mark> *Taught part of these modules take place in semester two, independent study continues into term three for students. Submission of work falls at the end of semester three.*	

Part Time Programme Structure for MSc Cybercrime and Digital Investigations		
Year 1		
<mark>Term One</mark> **(60 credits)**	<mark>Term Two</mark> **(60 credits)**	<mark>Term Three</mark> **(60 credits)**
15 CREDITS CST4230 Digital Forensics and Incident Management	**15 CREDITS** CST4220 Blockchain Anatomy and Analytics	
15 CREDITS	**15 CREDITS** CST4250 Open-source Intelligence Techniques	

4

CST4240 Financial Crime Risks from Emerging Technologies		
15 CREDITS CRM4615 Cybercrime and Society	**15 CREDITS** CRM4630 Text Mining and Analysis	
Year 2		
15 CREDITS CRM4629 Research Strategies in Social Sciences	**15 CREDITS** OPTIONAL MODULE	
	60 CREDITS CRM4617 Dissertation **OR** CRM4XXX Work-Based Experience *Taught part of these modules take place in semester two, independent study continues into term three for students. Submission of work falls at the end of semester three.*	

12.2 Levels and modules		
Level 7		
COMPULSORY	OPTIONAL *	PROGRESSION REQUIREMENTS

Students must take all of the following:	Students must also choose 1 from the following:	
CST4230 Digital Forensics and Incident Management CST4240 Financial Crime Risks from Emerging Technologies CST4220 Blockchain Anatomy and Analytics CST4250 Open-source intelligence Techniques CRM4615 Cybercrime and Society CRM4630 Text Mining and Analysis CRM4629 Research Strategies in Social Sciences CRM4617 Dissertation OR <mark>CRM4XXX Work-Based Experience</mark>	CRM4610 Advanced Research Strategies CRM4618 Drugs and Crime CRM 4625 Political Violence and Terrorism CRM4616 Cybercultures and Crime	

*Please refer to your programme page on the website re availability of option modules

12.3 Non-compensatable modules	
Module level	**Module code**
All level 7	CST4230 Digital Investigations and Incident Management CST4240 Financial Crime Risks from Emerging Technologies CST4220 Blockchain Anatomy and Analytics CST4250 Open-source intelligence Techniques CRM4615 Cybercrime and Society CRM4630 Text Mining and Analysis CRM4629 Research Strategies in Social Sciences CRM4617 Dissertation OR <mark>CRM4XXX Work-Based Experience</mark>

6

13. Information about assessment regulations

This programme will run in line with general University Regulations:
https://www.mdx.ac.uk/__data/assets/pdf_file/0031/623758/Regulations-2021-22-V1.12.pdf

14. Placement opportunities, requirements and support

Students may elect to undertake a 60-credit work-based experience module. The programme team and MDXWorks will be able to ==advise about placements in work settings== and may be able to link students with potential organisations. However, the process of researching, selecting, and negotiating the ==work-based experience== is a crucial element of the learning process and assessment and as such should be student led.

Students will be allocated with a university supervisor for the ==work-based experience==, and before enrolling on the module can seek advice and guidance from the employability lead for the department or module leader as well as the employability office and placement administrator. The module leader or employability office will assess students' application based on ==eligibility==, experience, interests, and general suitability.

15. Future careers / progression

This master's degree aims to develop social science graduates who have the skills needed to respond to cybercrime and e-security challenges, from issues relating to transnational crime, intellectual property, sexual offences, vulnerable victims, privacy legislation and law. Potential career paths include policy development, corporate security, e-investigation, social media safety, anti-money laundering (investigatory and other roles in the Financial Conduct Authority, Financial Services Ombudsman etc.), safeguarding, designing, and implementing data security and information strategies, analytics, business continuity and others.

Several major auditing firms also have graduate entry programmes that specifically identify criminology as a base qualification for applicants. Those already in the industry view their masters-level studies as a means of facilitating career progression within their organisations. Several students have continued their studies at doctoral level. Staff in the department will work alongside the employability office to facilitate your future career decisions. Some of our recent graduates have entered careers as Analysts, System Engineers, Risk and Compliance roles and work for the National Audit Office, BAE Systems and NHS.

16. Particular support for learning

- Programme induction workshop for all students within the first induction week.
- All academics in the department, including programme leaders provide up to four hours of office hours on a weekly basis which students can make use of without making an appointment.
- Availability of guidance from Graduate Academic Assistants.
- The Learner Enhancement Team (LET) can provide one-to-one tutorials and workshops for those students needing additional support with literacy and numeracy.
- Availability of guidance from library staff, including a dedicated Criminology Librarian.

- E-mail access to academics and support services.
- Comprehensive information in programme and module handbooks.
- Facilities and equipment available to assist students with disabilities.
- Access to careers information and an Employability Service staffed with careers advisers with extensive knowledge of career options in criminology.
- Middlesex University Library and subject librarian will provide access to specialist learning resources i.e., journals, textbooks, reports etc. For ease of access for students based at Hendon, the library has facilities for inter-library loans and photocopying of any articles required. The library can also provide texts/articles or chapters where possible in electronic format for students. Other articles may be obtained from the British Library in London where a similar provision is provided.
- MyLearning/Moodle provides additional information and resources to support students. Course materials, links to resources and interactive exercises are provided.
- Students may undertake a research project at their workplace where relevant and possible.
- UniHelp, university's central service through which students can access a range of support for the kinds of concerns that might arise throughout their study.
- Counselling and Mental Health Team – provides mental wellbeing support and a confidential individual counselling service to help students manage any challenges affecting them emotionally or psychologically that they might face during their study.
- Disability and Dyslexia Service – supporting an inclusive teaching and learning environment which caters for all students.
- Student Welfare Advice Team – providing information and advice on funding matters and housing.
- International Student Advice Team – providing information and advice on visa and immigration concerns, for both international applicants and current international students.
- Law Progression and Support Team – providing ongoing student support to ensure students' progress on their programme.

17. HECos code(s)	
18. Relevant QAA subject benchmark(s)	Criminology Benchmark Statement 2019

19. Reference points
The following reference points were applicable in the design of this programme:

- Middlesex University Regulations 2021-2022.
- QAA Subject Benchmark Statement: Criminology, 2019.
- Middlesex University, Inclusive Curriculum Paper.
- Principles of Blended Learning, Paper 2022.
- University Learning and Teaching policies and strategies.
- The QAA Quality Code for Higher Education, 2014.
- The QAA Characteristics Statement: Master's Degree, 2020.
- SEEC, Credit Level Descriptors for Higher Education, 2021.
- Business and Law Assessment Tariff Guidance, November 2021.

20. Other information

The availability of specific optional modules is subject to achieving appropriate student numbers. Modules with less than 10 students enrolled before the commencement of the first week of teaching are unlikely to run.

The Department of Criminology and Sociology at Middlesex University is part of the Common Studies Session in Critical Criminology (CSSCC) alongside different universities across Europe (i.e., Athens, Porto, Barcelona, Ghent, Hamburg, Rotterdam, Kent and John Jay College in New York). Criminology Masters students are encouraged to attend this bi-annual conference held in-person at one of the contributing partner universities for the vibrant exchange of ideas, debate, and networking opportunity.

Please note programme specifications provide a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve if s/he takes full advantage of the learning opportunities that are provided. More detailed information about the programme can be found in the rest of your programme handbook and the university regulations.

21. Curriculum map for MSc Cybercrime and Digital Investigations

This section shows the highest level at which programme outcomes are to be achieved by all graduates, and maps programme learning outcomes against the modules in which they are assessed.

Programme learning outcomes

Knowledge and understanding of:	
A1	Current theoretical and enforcement debates in cybercrime and the applicability of cybercrime research to criminological theory, practice, and policy.
A2	Contemporary methods in researching cybercrime.
A3	Range of tools and techniques to carry out a digital investigation.
A4	How technology facilitates and is used to respond to crime.
A5	Legal and professional issues related to computer-related crime, digital evidence, and digital forensic investigations.
A6	Challenges and opportunities presented by technologies for cyber analysts.
A7	Investigative guidelines, and ethical research practices and legislation.
Skills to:	
B1	Use relevant tools and techniques to carry out digital investigations.
B2	Investigate, collect, analyse, and present relevant digital evidence from computing devices.
B3	Advise on managing compliance in corporate environments and implementing tools and techniques for detecting, investigating, and preventing financial crime.
B4	Evaluate new sources of research knowledge and information and those used in previous research.
B5	Effectively develop and design a research proposal.
B6	Use learning resources effectively in relation to researching cybercrime.
B7	Criticise and engage in reasoned debate about relevant ethical digital investigation issues.
B8	Plan and carry out an independent project, evaluation of a placement or work-based development project.

Programme outcomes														
A1	A2	A3	A4	A5	A6	A7	B1	B2	B3	B4	B5	B6	B7	B8
Highest level achieved by all graduates														
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7

Module Title	Module Code by Level	A1	A2	A3	A4	A5	A6	A7	B1	B2	B3	B4	B5	B6	B7	B8
Blockchain Anatomy and Analytics	CST4220	X			X		X		X		X				X	
Digital Forensics and Incident Management	CST4230			X	X		X	X	X	X						X	
Financial Crime Risks from Emerging Technologies	CST4240	X			X		X	X			X	X			X	
Open-source intelligence Techniques	CST4250		X	X	X		X	X		X					X	
Cybercrime and Society	CRM4615	X			X	X	X		X			X		X	X	
Text Mining and Analysis	CRM4630	X	X	X		X	X	X	X	X		X	X	X	X	
Research Strategies in Social Sciences	CRM4629		X	X				X				X	X	X	X	
Dissertation	CRM4617	X	X	X	X	X		X		X	X	X	X	X	X	X
<mark>Work Based Experience</mark>	<mark>CRM4XXX</mark>	X		X	X	X		X		X	X	X		X	X	X
Advanced Research Strategies	CRM4610	X	X	X		X		X		X		X		X	X	
Drugs and Crime	CRM4618	X						X				X			X	
Political Violence and Terrorism	CRM4625	X										X				
Cybercultures and Crime	CRM4616	X			X	X	X					X		X	X	