LLM in Cybersecurity and Emerging Technologies

Programme specification document

Awarding institution	Bath Spa University
Teaching institution	Bath Spa University
School	Business School
Main campus	Newton Park
Other sites of delivery	N/A
Other Schools involved in delivery	N/A
Name of award(s)	LLM Cybersecurity and Emerging Technologies
Qualification (final award)	LLM
Intermediate awards available	PgCert
Routes available	Single/Joint
Duration of award	1-year full time, 2 years part-time
Sandwich period	Optional
Modes of delivery offered	Campus-based
Regulatory Scheme[1]	Taught Postgraduate Academic Framework
Professional, Statutory and Regulatory Body accreditation	N/A
Date of most recent PSRB approval (month and year)	
Renewal of PSRB approval due (month and year)	
UCAS code	N/A
Route code (SITS)	N/A
Relevant QAA Subject Benchmark Statements (including date of publication)	QAA Subject Benchmark Statement: Law (08th March 2023) QAA Characteristics Statement: Master's Degree (08th March 2023) QAA Subject Benchmark Statement: Master's Degree in Business & Management (08th March 2023)
Date of most recent approval	September 2024
Date specification last updated	June 2024

[1] This should also be read in conjunction with the University's Qualifications Framework

Programme Overview

The LLM Cybersecurity and Emerging Technologies programme provides students with advanced knowledge and a comprehensive understanding of the intricate legal frameworks governing cybersecurity and the rapidly evolving field of technology. Through an in-depth examination of the laws, rules, and regulations governing various aspects of cybersecurity and technology, students enhance their expertise in this specialised area of law.

This programme equips students with core legal knowledge and fundamental principles, essential for pursuing careers in legal practice, public sector organisations, non-governmental organisations, multinational corporations, and other entities both domestically and internationally. Emphasising practical application, the curriculum includes practice-led exercises, some in collaboration with external organisations, ensuring students gain valuable real-world experience.

A notable aspect of the programme is its emphasis on contemporary issues such as data protection, cybercrime, cyber war, artificial intelligence, digital privacy, and the ethical implications of emerging technologies. By analysing domestic and international regulations addressing these challenges, students develop the capacity to address pressing global issues through a legal perspective.

Throughout the programme, students engage in high-level abstract thinking, fostering critical responses and innovative approaches within the realm of cybersecurity and technology law. This analytical capability is crucial for legal professionals aspiring to influence policy and drive change in the global digital landscape.

Employing a holistic and individualised approach, the LLM Cybersecurity and Emerging Technologies programme nurtures both academic and practical skill development alongside personal and professional growth. Tailoring the learning experience to each student’s unique journey ensures graduates are well-prepared to excel in various professional settings. This comprehensive programme enhances employability and positions graduates as leaders capable of navigating and shaping the evolving field of cybersecurity and technology law.

Programme Aims

1. Provide students with an advanced understanding of the legal frameworks, principles, and challenges surrounding cybersecurity and emerging technologies within a global context.
2. Develop students’ ability to critically analyse and evaluate complex legal issues, regulations, and policies related to cybersecurity, data protection, digital privacy, and the ethical implications of emerging technologies.
3. Equip students with the skills necessary to apply legal knowledge effectively in practical scenarios, including legal practice, policymaking, corporate governance, and technology management.

4. Cultivate students' expertise in the specialised areas of cybersecurity law, cybercrime regulation, digital innovation, and the legal implications of emerging technologies such as artificial intelligence, blockchain, and the Internet of Things.
5. Enhance students' professional skills, including critical thinking, problem-solving, communication, and teamwork, to prepare them for diverse career pathways in legal practice, government agencies, multinational corporations, technology firms, consulting, academia, and non-governmental organisations.
6. Encourage students to engage in advanced research and scholarship, promoting innovative thinking and contributing to the advancement of knowledge in the fields of cybersecurity, technology law, and digital governance.
7. Instil a commitment to lifelong learning and professional development, empowering students to adapt to evolving legal, technological, and societal changes throughout their careers.

Programme Intended Learning Outcomes (ILOs)
(NB These ILOs are at level 7 of the FHEQ)

<u>A Subject-specific Skills and Knowledge</u>

A1 Systematic Problem-Solving: Systematically resolve legal issues in cybersecurity and emerging technologies, considering international legal frameworks and their impact on technology law.
A2 Critical Evaluation: Critically assess legal dynamics in cybersecurity and emerging technologies, including the role of domestic, regional, and international institutions.
A3 Application of Norms: Apply global norms to cybersecurity and emerging technology cases, addressing challenges through practical exercises.
A4 Self-Reflection and Creativity: Demonstrate this by applying self-reflection and creativity when addressing the legal complexities in cybersecurity and emerging technologies.
A5 Research Methodologies: Evaluate legal research methodologies relevant to cybersecurity and emerging technologies.
A6 Independent Learning and Communication: Apply independent learning and effective communication skills suitable for cybersecurity and emerging technology contexts.
A7 Diversity and Ethics: Apply an understanding of social justice and ethics principles, and value diversity in cybersecurity and technology law.

B Cognitive and Intellectual Skills

B1: Analyse and evaluate complex legal issues and challenges specific to cybersecurity and emerging technologies, demonstrating a logical and systematic approach.
B2: Critically reflect on and address ethical dilemmas arising from the intersection of law, cybersecurity, and emerging technologies at local, national, and global levels.
B3: Proficiently manage and interpret intricate and relevant information and evidence in cybersecurity contexts, making informed judgments and recommendations.
B4: Conduct comprehensive and original independent research in cybersecurity law and emerging technologies, applying advanced research methodologies to create and interpret legal knowledge effectively.

C Skills for Life and Work

C1 Autonomous learning (including time management) that demonstrates the exercise of initiative, personal responsibility and decision-making in complex and unpredictable situations and the independent learning ability required for continuing professional development

C2 Team working skills necessary to succeed in the global workplace, with an ability both to work in and lead teams effectively, as well as the ability to act autonomously in planning and implementing tasks at a professional or equivalent level

C3 Communication skills that show the ability to communicate clearly to specialist and non-specialist audiences knowledge at, or informed by, the forefront of the academic discipline, field of study or area of professional practice, and the conclusions drawn from dealing with complex issues systematically

C4 IT skills and digital literacy that demonstrate the ability to develop new skills to a high level and to approach complex issues systematically and creatively

PgCert Intended Learning Outcomes

A. Subject-specific Skills and Knowledge
A1-4
B. Cognitive and Intellectual Skills
B1-3
C. Skills for Life and Work
C1-4

PgDip Intended Learning Outcomes

A. Subject-specific Skills and Knowledge
A1-4
B. Cognitive and Intellectual Skills
B1-3

C. Skills for Life and Work
C1-4

Programme content

This programme comprises the following modules.

Key:
Core = C
Required = R
Required* = R*
Optional = O
Not available for this status = N/A
If a particular status is greyed out, it is not offered for this programme.

Subject offered as single and/or joint programme

LLM Cybersecurity and Emerging Technologies				Status	
Level	Code	Title	Credits	Single	Joint
Core Modules					
7	LAW7110-60	Legal Research Project	60	R*	
7	LAW7109-60	Legal Clinic	60	R*	
7	LAW7205-15	Entertainment, Media and Intellectual Property Law	15	C	
7	CYS7000-30	Cybersecurity bootcamp	30	C	
7	LAW7204-15	Cyber Space Law	15	C	
7	CYS7005-15	Cyberwar	15	O	
7	LAW7206-15	Competition Law	15	O	
7	LAW7107-15	Business Law and Practice	15	O	
7	LAW7207-15	Cyber Security Law & Fraud Analytics	15	O	
7	LAW7208-15	Artificial Intelligence Law	15	O	

Assessment methods

A range of summative assessment tasks will be used to test the Intended Learning Outcomes in each module. These are indicated in the attached assessment map which shows which tasks are used in which modules.

Students will be supported in their development towards summative assessment by appropriate formative exercises.

Please note: if you choose an optional module from outside this programme, you may be required to undertake a summative assessment task that does not appear in the assessment grid here in order to pass that module.

Work experience and placement opportunities.

The LLM programme in Cybersecurity and Emerging Technologies is designed to enhance student employability and ensure a student-centric focus. In addition to the comprehensive curriculum, students will have the option to participate in work experience, portfolio development, and a Cybersecurity bootcamp. These components are integral to the programme and aim to provide practical skills and real-world experience.

Through the Legal Clinic and Legal Research Project modules, students will have opportunities for practical work experience and engagement with regional organisations. These modules are specifically designed to offer hands-on experience in legal practice, allowing students to apply their academic knowledge in real-world settings. This engagement will help students build professional networks, gain valuable insights into the cybersecurity industry, and develop skills that are highly sought after by employers.

Students will have numerous opportunities to engage with relevant stakeholders during curricular and co-curricular activities. Activities such as debating and public speaking will be available, offering students the chance to enhance their advocacy, problem-solving, communication, teamwork, and writing skills. These activities enrich the learning experience and play a crucial role in preparing students for successful careers in cybersecurity and related fields.

The Cybersecurity bootcamp is a key element of the programme, providing intensive, hands-on training that enhances students' practical skills and employability. This bootcamp allows students to work on real-life cybersecurity challenges and collaborate with experts in the field.

This programme is committed to providing a well-rounded education that balances academic rigour with practical experience. This, in turn, fosters employability and ensures that students are well-equipped for their future careers.

Table of Additional Course Costs

Module Code & Title	Type of Cost	Cost
n/a		

Graduate Attributes

	Bath Spa Graduates…	In the LLM Cybersecurity and Emerging Technologies, we enable this…

1	Will be employable: equipped with the skills necessary to flourish in the global workplace, able to work in and lead teams	by providing students with opportunities for work-related experience and the development of transferable skills essential for future legal and professional practice. This programme is designed to equip students with practical knowledge and hands-on experience, fostering skills that are highly valued in the legal and cybersecurity sectors. Through internships, simulations, and industry collaborations, students gain real-world insights and competencies, preparing them for successful careers in a variety of professional settings.
2	Will be able to understand and manage complexity, diversity and change	by providing students with a robust emphasis on nurturing an international focus and an interdisciplinary approach, we enhance their employability skills. Students acquire a comprehensive skill set essential for thriving in today's interconnected world by integrating global perspectives and drawing from various disciplines. Through collaboration in multicultural teams addressing diverse and intricate problems, students learn to navigate differing viewpoints and cultures, refining their abilities to identify, plan, and implement effective solutions, decisions, and judgments. This immersive learning experience prepares students for the intricacies of the legal and cybersecurity landscapes and fosters the adaptability and cross-cultural competencies required for success in a diverse and dynamic professional environment.
3	Will be creative: able to innovate and to solve problems by working across disciplines as professional or artistic practitioners	by providing students with engagement across legal, business, and management disciplines in the realm of LLM Cybersecurity and Emerging Technologies, they gain exposure to a wide array of knowledge and viewpoints. For example, students can examine case studies that assess cybersecurity regulations within multinational tech companies, necessitating an understanding of both legal frameworks and technological implications. These projects foster critical and creative thinking among students, allowing them to apply their diverse skill sets to tackle intricate challenges and implement effective solutions in various cybersecurity contexts. This hands-on, interdisciplinary approach to learning equips students with the practical expertise and flexibility necessary to excel in the dynamic field of cybersecurity law and emerging technologies.
4	Will be digitally literate: able to work at the	by providing students with facilitated interaction with diverse digital resources throughout the programme,

	interface of creativity and technology	we encompass immersive skills simulations, dynamic online assessments, and the integration of multimedia tools to enrich the learning experience. These resources enable students to actively develop and refine their digital skill set, which is a crucial asset in today's technology-driven professional landscape. Moreover, this approach equips students with practical, hands-on experience in utilising digital platforms commonly employed in legal practice, thereby enhancing their readiness for the demands of the modern workplace.
5	Will be internationally networked: either by studying abroad for part of the their programme, or studying alongside students from overseas	by providing students with a scholarly setting that embraces multiculturalism, they will hone their intercultural awareness through collaborating with students from diverse countries and cultures. For instance, interacting with a teammate from Nigeria during a project may reveal their emphasis on harmony and consensus-building in teamwork, contrasting with the more individualistic approach often found in Western cultures.
6	Will be creative thinkers, doers and makers	by providing students with opportunities to foster creativity, cultivate sharp judgment, and equip themselves to address cybersecurity, emerging technologies, and innovation-related challenges, we empower them to refine their ability to identify and resolve legal issues within these dynamic fields. This includes evaluating alternative approaches and assessing associated risks. For example, imagine being tasked with a case involving the drafting of contractual agreements for a novel tech venture. Here, students would be encouraged to think innovatively, exploring diverse legal strategies to safeguard the interests of cybersecurity and emerging technology advancements. Moreover, they would apply analytical skills to decipher market dynamics and technological trends, ensuring that the proposed legal framework aligns with the objectives of cybersecurity and emerging technologies. Through this process, students provide insightful legal advice, recommending the most advantageous legal pathways to optimise outcomes in cybersecurity and emerging technology endeavours.
7	Will be critical thinkers: able to express their ideas in written and oral form, and	by providing students with an LLM in cybersecurity and emerging technologies, they will be equipped with both theoretical knowledge and practical skills to proficiently identify legal challenges. They can apply relevant principles, rules, theories, and

	possessing information literacy	methodologies to devise solutions and offer guidance. For example, when tackling an intricate case related to a cybersecurity breach in a technological infrastructure, students can leverage their comprehension of cybersecurity law. They will scrutinise the legal frameworks, pertinent regulations, and precedents to ascertain liability and evaluate potential remedies. Subsequently, they will provide strategic legal advice to address the situation, delineating the most suitable legal strategies to protect interests and minimise adverse impacts.
8	Will be ethically aware: prepared for citizenship in a local, national and global context	by providing students with opportunities to enhance their understanding of the intersection between law and morality, they can recognise the paramount importance of ethics in cybersecurity, legal frameworks, and professional conduct. For instance, as experts in cybersecurity and law, students may encounter scenarios where clients suggest lucrative yet ethically dubious business ventures. Understanding the ramifications of such decisions from both legal and moral perspectives is essential for making informed choices and upholding ethical standards in professional endeavours.

Modifications

Module-level modifications

Code	Title	Nature of modification	Date(s) of approval and approving bodies	Date modification comes into effect
N/A	N/A	N/A	N/A	N/A

Programme-level modifications

Nature of modification	Date(s) of approval and approving bodies	Date modification comes into effect
N/A	N/A	N/A

Attached as appendices:

1. Programme structure diagram
2. Map of module outcomes to level/programme outcomes
3. Assessment map
4. Module descriptors

Appendix 1: Programme Structure Diagram – LLM Cybersecurity and Emerging Technologies

Full-Time (One Year)		
Level 7		
Trimester 1	**Trimester 2**	**Trimester 3**
Core Modules		
CYS7000-30 Cybersecurity Bootcamp	LAW7205-15 Entertainment, Media and Intellectual Property Law	
	LAW7204-15 Cyber Space Law	
Required* Modules		
		LAW7110-60 Legal Research Project
		LAW7109-60 Legal Clinic
Optional Modules		
LAW7207-15 Cyber Security Law & Fraud Analytics	LAW7208-15 Artificial Intelligence Law	
LAW7206-15 Competition Law	LAW7107-15 Business Law and Practice	
	CYS7005-15 Cyberwar	
Rule Notes: Students must choose 1 x 60-credit R* module and 4 x 15-credit Optional modules. *****BM7032-15 Advanced Academic and Business Skills is recommended for International students whose first language is <u>not</u> English.		

Appendix 2: Map of Intended Learning Outcomes

Level	Module Code	Module Title	Status (C,R,R*,O)[4]	Subject-specific Skills and Knowledge							Skills for Life and Work						
				A1	A2	A3	A4	A5	A6	A7	B1	B2	B3	C1	C2	C3	C4
7	LAW7110-60	Legal Research Project	R*	X		X		X	X		X			X	X		X
7	LAW7109-60	Legal Clinic	R*		X	X		X		X		X		X			X
7	LAW7205-15	Entertainment, Media and Intellectual Property Law	C	X		X	X	X	X		X		X		X	X	
7	CYS7000-30	Cybersecurity Bootcamp	C		X	X	X		X		X			X		X	X
7	LAW7204-15	Cyber Space Law	C		X		X	X		X	X		X		X	X	
7	CYS7005-15	Cyberwar	O	X		X	X	X	X		X	X		X			X
7	LAW7206-15	Competition Law	O	X	X		X		X	X	X		X	X		X	X
7	LAW 7107-15	Business Law and Practice	O	X		X	X	X		X	X	X	X		X		X

7	LAW7207-15	Cyber Security Law & Fraud Analytics	O	X	x		x		X	X		x		x		x	
7	LAW7208-15	Artificial Intelligence Law	O	X		X		X		X	X	X		X		X	

[4] C = Core; R = Required; R* = Required*; O = Optional

Appendix 3: Map of Summative Assessment Tasks by Module

Level	Module Code	Module Title	Status (C,R,R*, O)[5]	Assessment method								
				Coursework				Practical			Written Examination	
				Case Study	Dissertation	Essay	Report	Practical Project	Presentation	Portfolio	Time Constrained Assessment	Written Assessment
7	LAW7110-60	Legal Research Project	C		X							
7	LAW7109-60	Legal Clinic	C							X		
7	CYS7000-30	Cybersecurity Bootcamp	C						X	X		
7	LAW7204-15	Cyber Space Law	C					X				
7	LAW7205-15	Entertainment, Media and Intellectual Property Law	C				X					
7	CYS7005-15	Cyberwar	O	X								
	LAW7206-15	Competition Law	O			X						

	LAW 7107-15	Business Law and Practice	O	X								
7	LAW7207-15	Cyber Security Law & Fraud Analytics	O						X			
7	LAW7208-15	Artificial Intelligence Law	O				X					

[5] C = Core; R = Required; R* = Required*; O = Optional

The Map of Summative Assessment Tasks by Module illustrates the various assessment options available for each module. This map highlights the flexibility of the programme in offering diverse assessment methods, which are designed to enhance students' employability skills. By incorporating a range of evaluation techniques, the programme ensures that students develop a comprehensive skill set that is highly valued in the professional legal environment.