UNIVERSITY OF WOLVERHAMPTON

Course Specification

Published Date:	21-Aug-2026
Produced By:	Multi Type Usr Record For All Personnel
Status:	Validated

Core Information

Awarding Body / Institution:	University of Wolverhampton		
School / Institute:	School of Architecture, Computing and Engineering		
Course Code(s):	CS068P01UM CS068P31UM	Full-time Part-time	15 Months 28 Months
Course Title:	MSc Cyber Security and Artificial Intelligence		
Hierarchy of Awards:	Master of Science Cyber Security and Artificial Intelligence		
Language of Study:	English		
Date of first cohort:	14/Sep/2026		
Specification valid from:	2025/6		

Academic Staff

Course Leader:	Zeeshan Ahmad
Head of Department:	

Course Information

Location of Delivery:	University of Wolverhampton
Category of Partnership:	Standard Provision (Not delivered in partnership)
Teaching Institution:	University of Wolverhampton
Open / Closed Course:	This course is open to all suitably qualified candidates.

Entry Requirements:

Entry requirements are subject to regular review. The entry requirements applicable to a particular academic year will be published on the University website (and externally as appropriate e.g. UCAS

This is a conversion MSc. It is aimed at graduates from a wide range of disciplines who wish to develop knowledge and skills in cyber security and artificial intelligence for professional careers in these areas. Minimum entry requirements are

1. A lower second-class honours degree in any discipline.
1. GCSE Grade 4 in Mathematics (formerly Grade C) or equivalent

If applicants do not hold a GCSE Grade 4 in Mathematics or equivalent, then they have the option of completing the University's GCSE Mathematics Equivalence course to meet this requirement.

Alternatively:

Applicants with relevant industrial experience will also be considered. An interview process may also be used to assess suitability for the course for candidates with non-standard academic backgrounds but with demonstrable industry experience.

International Applicants

Qualifications must be deemed equivalent to the above entry requirements.

1. English Language requirements are normally IELTS 6.0 with a minimum of 5.5 in each area (unless otherwise stated) or equivalent accepted qualification https://www.wlv.ac.uk/international/making-an-application/language-entry-requirements/
1. Please use the following link https://www.wlv.ac.uk/international/ to see the range of English Language Pre-Sessional courses and related Pre-MSc courses offered by the University of Wolverhampton International Academy.
1. For further information relating to overseas qualification, please use the following link https://www.wlv.ac.uk/international/our-locations/your-country/

Distinctive Features of the Course:

MSc Cyber security and Artificial Intelligence course is designed for students who want to develop expertise at the intersection of two of the most important and fast-moving areas in computing. As organisations increasingly rely on intelligent, connected and data-driven systems, there is growing demand for professionals who can understand both how to secure digital environments and how to apply artificial intelligence responsibly and effectively. This course is distinctive because it brings these two areas together in a single postgraduate programme, helping you develop a broader and more future-focused skill set than a traditional single-subject degree.

The course combines strong foundations in cyber security and artificial intelligence (AI) with practical, applied learning. Students will study information assurance, secure infrastructure, ethical hacking, AI, deep machine learning, incident management and response, and Generative AI for cybersecurity. This gives you the opportunity to understand both the technical principles and the real-world challenges involved in protecting modern digital systems. You will also explore how AI can be used within cyber security contexts, while developing awareness of ethics, professional responsibility and the wider impact of digital technologies.

Throughout the course, learning is connected to realistic technical tasks, case studies and applied problem solving. This helps you build confidence in using tools, methods and techniques relevant to contemporary cyber security and AI practice. By the end of the course, you will have developed advanced knowledge, practical ability and independent research skills that support further study or a wide range of careers in cyber security, AI and related digital fields.

Distinctive features include:

- A combined focus on cyber security and artificial intelligence within one postgraduate degree.
- Specialist study in areas such as ethical hacking, secure infrastructure, AI, incident management and response, and generative AI for cybersecurity.
- A curriculum that reflects both technical depth and broader professional issues such as ethics, governance and responsible practice.
- Practical learning through labs, case studies, technical tasks and project-based work.
- Opportunities to explore how AI can be applied within cyber security settings and challenges.
- Research-informed teaching that supports critical thinking, enquiry and independent learning.
- A substantial dissertation that allows you to investigate a specialist topic aligned with your interests and career goals.
- Preparation for a wide range of roles across cyber security, AI, digital risk, technical operations and related areas.

Intakes:

September
November
January
March

Major Source of Funding:

Office for Students (OFS)

Tuition Fees:

Tuition fees are reviewed on an annual basis. The fees applicable to a particular academic year will be published on the University website.

Year	Status	Mode	Amount
2026/7	H	Full Time	£11015.00
2026/7	Overseas	Full Time	£18645.00
2026/7	H	31	£5508.00

PSRB:

None

Course Structure:

January (Full-time)

Module	Title	Credits	Period	Type
7CS136	Ethical Hacking	15	INYR	Core
7CS124	Incident Management and Response	15	INYR	Core
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS122	Research Methods & Professionalism	15	INYR	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CS136	Ethical Hacking	15	INYR	Core
7CS122	Research Methods & Professionalism	15	INYR	Core

January (Full-time)

Module	Title	Credits	Period	Type
7CS126	Principles of Artificial Intelligence	15	INYR	Core
7CS141	Information Assurance	15	INYR	Core
7CS127	Deep Machine Learning	15	INYR	Core
7CS129	Secure Infrastructure	15	INYR	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CS141	Information Assurance	15	INYR	Core
7CS129	Secure Infrastructure	15	INYR	Core

January (Full-time)

Module	Title	Credits	Period	Type
7CS139	Computer Science Dissertation	60	INYR	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS124	Incident Management and Response	15	INYR	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CS126	Principles of Artificial Intelligence	15	INYR	Core
7CS127	Deep Machine Learning	15	INYR	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CS139	Computer Science Dissertation	60	INYR	Core

March (Full-time)

Module	Title	Credits	Period	Type
7CS124	Incident Management and Response	15	INYR	Core
7CS122	Research Methods & Professionalism	15	INYR	Core

March (Part-time)

Module	Title	Credits	Period	Type
7CS122	Research Methods & Professionalism	15	INYR	Core

March (Full-time)

Module	Title	Credits	Period	Type
7CS126	Principles of Artificial Intelligence	15	INYR	Core
7CS141	Information Assurance	15	INYR	Core
7CS127	Deep Machine Learning	15	INYR	Core
7CS129	Secure Infrastructure	15	INYR	Core
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS136	Ethical Hacking	15	INYR	Core

March (Part-time)

Module	Title	Credits	Period	Type
7CS141	Information Assurance	15	INYR	Core
7CS129	Secure Infrastructure	15	INYR	Core
7CS136	Ethical Hacking	15	INYR	Core

March (Full-time)

Module	Title	Credits	Period	Type
7CS139	Computer Science Dissertation	60	INYR	Core

March (Part-time)

Module	Title	Credits	Period	Type
7CS124	Incident Management and Response	15	INYR	Core

March (Part-time)

Module	Title	Credits	Period	Type
7CS126	Principles of Artificial Intelligence	15	INYR	Core
7CS127	Deep Machine Learning	15	INYR	Core
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core

March (Part-time)

Module	Title	Credits	Period	Type
7CS139	Computer Science Dissertation	60	INYR	Core

September (Full-time)

Module	Title	Credits	Period	Type
7CS126	Principles of Artificial Intelligence	15	INYR	Core
7CS141	Information Assurance	15	INYR	Core
7CS127	Deep Machine Learning	15	INYR	Core
7CS129	Secure Infrastructure	15	INYR	Core
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS136	Ethical Hacking	15	INYR	Core
7CS122	Research Methods & Professionalism	15	INYR	Core
7CS124	Incident Management and Response	15	INYR	Core

September (Part-time)

Module	Title	Credits	Period	Type
7CS141	Information Assurance	15	INYR	Core
7CS129	Secure Infrastructure	15	INYR	Core
7CS136	Ethical Hacking	15	INYR	Core
7CS122	Research Methods & Professionalism	15	INYR	Core

September (Full-time)

Module	Title	Credits	Period	Type
7CS139	Computer Science Dissertation	60	INYR	Core

September (Part-time)

Module	Title	Credits	Period	Type
7CS126	Principles of Artificial Intelligence	15	INYR	Core
7CS127	Deep Machine Learning	15	INYR	Core
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS124	Incident Management and Response	15	INYR	Core

September (Part-time)

Module	Title	Credits	Period	Type
7CS129	Secure Infrastructure	15	INYR	Core

November (Full-time)

Module	Title	Credits	Period	Type
7CS127	Deep Machine Learning	15	INYR	Core
7CS129	Secure Infrastructure	15	INYR	Core
7CS136	Ethical Hacking	15	INYR	Core
7CS124	Incident Management and Response	15	INYR	Core
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS122	Research Methods & Professionalism	15	INYR	Core

November (Part-time)

Module	Title	Credits	Period	Type
7CS129	Secure Infrastructure	15	INYR	Core
7CS136	Ethical Hacking	15	INYR	Core
7CS122	Research Methods & Professionalism	15	INYR	Core

November (Full-time)

Module	Title	Credits	Period	Type
7CS126	Principles of Artificial Intelligence	15	INYR	Core
7CS141	Information Assurance	15	INYR	Core

November (Part-time)

Module	Title	Credits	Period	Type
7CS141	Information Assurance	15	INYR	Core

November (Full-time)

Module	Title	Credits	Period	Type
7CS139	Computer Science Dissertation	60	INYR	Core

November (Part-time)

Module	Title	Credits	Period	Type
7CS127	Deep Machine Learning	15	INYR	Core
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS124	Incident Management and Response	15	INYR	Core

November (Part-time)

Module	Title	Credits	Period	Type
7CS126	Principles of Artificial Intelligence	15	INYR	Core

November (Part-time)

Module	Title	Credits	Period	Type
7CS139	Computer Science Dissertation	60	INYR	Core

Please note: Optional modules might not run every year, the course team will decide on an annual basis which options will be running, based on student demand and academic factors, to create the best learning experience.

Learning, Teaching and Assessment

Regulations Exemption:

Exemption from the University's standard academic framework 1.3.1 allowing for the use of 15 credits modules taught modules at Level 7.

Reference Points:

UK Quality Code for Higher Education

Qualifications and Credit Frameworks

Subject Benchmark Statements

University Policies and Regulations

Equality Act 2010: guidance - GOV.UK

Apprenticeship Standard

Overview of Assessment:

Learning Outcomes	Modules
PGCERT01 Critically evaluate and apply current theories, concepts and principles in cyber security and artificial intelligence (AI) within academic and professional contexts. (Knowing)	7CS124 Incident Management and Response 7CS126 Principles of Artificial Intelligence 7CS127 Deep Machine Learning 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
PGCERT02 Demonstrate knowledge and practical skills in core areas of cyber security and AI. (Knowing)	7CS124 Incident Management and Response 7CS126 Principles of Artificial Intelligence 7CS127 Deep Machine Learning 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance

Learning Outcomes	Modules
PGCERT03 Analyse technical problems, make informed decisions on complex issues, and communicate conclusions clearly to different audiences. (Doing)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
PGCERT04 Demonstrate self-direction in tackling cyber security and AI-related problems and take responsibility for planning and completing tasks effectively. (Doing)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS127 Deep Machine Learning 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity
PGCERT05 Review your work and identify strengths, limitations, and areas for improvement in cyber security and AI tasks. (Being)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS127 Deep Machine Learning 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
PGCERT06 Recognise your current knowledge and skills in cyber security and AI and identify areas for further development. (Being)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS126 Principles of Artificial Intelligence 7CS127 Deep Machine Learning 7CS129 Secure Infrastructure 7CS137 Generative AI and Automation for Cybersecurity
PGDIP01 Critically evaluate current theories, concepts and practices in cyber security and AI, informed by developments at the forefront of the wider computing discipline and professional practice. (Knowing)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS126 Principles of Artificial Intelligence 7CS127 Deep Machine Learning 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
PGDIP02 Demonstrate in-depth knowledge and practical and professional skills in cyber security, AI, and their application to modern digital systems. (Knowing)	7CS124 Incident Management and Response 7CS126 Principles of Artificial Intelligence 7CS127 Deep Machine Learning 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
PGDIP03 Analyse and respond to complex technical and professional issues in cyber security and AI and communicate conclusions clearly to different audiences using appropriate academic, technical and professional conventions. (Doing)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS127 Deep Machine Learning 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance

Learning Outcomes	Modules
PGDIP04 Demonstrate self-direction and originality in tackling and solving cyber security and AI-related problems, acting independently in the planning and implementation of tasks at a professional level. (Doing)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS127 Deep Machine Learning 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity
PGDIP05 Critically reflect on your learning, performance and decision making, and use this reflection to improve your practice. (Being)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity
PGDIP06 Reflect on your achievements and plan for future career development or further study in cyber security, AI, and related areas. (Being)	7CS122 Research Methods & Professionalism
MA01 Demonstrate a systematic understanding of knowledge, and a critical awareness of current challenges, risks, methods and new insights in cyber security and AI, informed by developments at the forefront of the broader computing discipline, field of study and professional practice. (Knowing)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS126 Principles of Artificial Intelligence 7CS127 Deep Machine Learning 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS139 Computer Science Dissertation 7CS141 Information Assurance
MA02 Show originality in the application of cyber security and AI knowledge, together with a practical understanding of how research, enquiry and technical investigation are used to create and interpret knowledge in the broader computing discipline. (Knowing)	7CS122 Research Methods & Professionalism 7CS127 Deep Machine Learning 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS139 Computer Science Dissertation
MA03 Deal with complex issues systematically and creatively, make sound judgements in the absence of complete data, and communicate conclusions clearly to specialist and non-specialist audiences. (Doing)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS127 Deep Machine Learning 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS139 Computer Science Dissertation 7CS141 Information Assurance
MA04 Demonstrate self-direction and originality in tackling and solving cyber security and AI-related problems, and act autonomously in planning and implementing tasks at a professional or equivalent level. (Doing)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS127 Deep Machine Learning 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS139 Computer Science Dissertation
MA05 Exercise initiative, personal responsibility and informed decision making in complex and unpredictable situations. (Being)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS139 Computer Science Dissertation
MA06 Continue to advance your knowledge and understanding through independent learning, professional development and the acquisition of new skills to a high level. (Being)	7CS122 Research Methods & Professionalism 7CS139 Computer Science Dissertation

Teaching, Learning & Assessment Strategy/(Learning and Teaching):

Our MSc Cyber Security and Artificial Intelligence course is taught through a balance of clear explanation, practical application and independent learning. The course

is designed to help you build knowledge step by step. You will first develop strong foundations in key areas of cyber security, artificial intelligence. As the course progresses, you will move into more advanced topics such as ethical hacking, generative AI for cybersecurity, incident management and response, and independent project work.

Teaching is delivered through a mix of lectures, seminars, workshops, lab sessions and guided independent study. Lectures introduce key concepts and give you the theoretical grounding needed for postgraduate study. Workshops and lab sessions help you apply that learning to practical tasks, technical problems and real-world case studies. This means you will not only learn the theory behind cyber security and AI, but also how to use tools, methods and techniques in practice.

The course is designed to support different ways of learning. In-person sessions give you opportunities for discussion, collaboration and hands-on work. Online materials support preparation, revision and follow-up study, helping you review ideas in your own time and manage your learning effectively. Across the modules, you will also develop important postgraduate skills such as critical thinking, research, problem solving, communication and independent learning.

Professional practice is embedded throughout the course. You will engage with realistic technical tasks, security scenarios, applied AI activities and project-based work that reflect current industry and research challenges. Through Research Methods and Professionalism, and through your wider module activities, you will also develop awareness of ethics, professional standards and responsible practice.

The course encourages you to become confident in using digital tools and technologies in a thoughtful and responsible way. By the end of your studies, you will be better prepared to work with both cyber security and AI in professional, technical and research settings.

Assessment Methods/Assessments:

The MSc Cyber Security and Artificial Intelligence course is designed to support your learning, build confidence and reflect the kinds of tasks you are likely to meet in professional practice. There are no formal closed-book exams on the course. Instead, assessment is mainly through coursework, which allows you to show your knowledge, technical skills and professional understanding in applied and meaningful ways. This also helps create a more manageable pattern of assessment across the course.

You can expect a range of assessment types, including technical reports, practical tasks, case study analysis, project work, presentations and research-based assignments, leading to your final dissertation. These methods allow you to demonstrate how you can apply cyber security and AI techniques, analyse problems, evaluate evidence, design solutions and communicate your work clearly. Assessment is designed not only to test what you know, but also to develop critical thinking, problem solving, independent enquiry and sound technical judgement.

Many modules include formative or developmental activities in the early stages. These give you the chance to test your understanding, receive feedback and improve your work before final submission. This helps you become familiar with master’s level expectations and supports steady progress across the course.

Assessment is also designed to be inclusive and accessible. A variety of formats are used so that you can demonstrate your strengths in different ways. Clear guidance, marking criteria and structured support are provided to help you understand what is expected and how to succeed. In some modules, you may also have opportunities to focus on topics, case studies or problem areas that connect with your interests and career goals.

Many assessments are linked to realistic technical and professional contexts. You may be asked to work on practical cyber security scenarios, AI-based problem-solving tasks, security analysis, system evaluation or applied project work. This helps ensure that assessment supports both academic success and professional readiness.

Further Information for Student:

Our MSc Cyber Security and Artificial Intelligence course has been designed to help you settle quickly into postgraduate study and build confidence from the start of the course. We recognise that students join from different academic, professional and cultural backgrounds. For that reason, the course is structured to support a smooth transition into Level 7 study. Early modules provide a strong foundation in both cyber security and artificial intelligence, helping you to understand key concepts, practical tools, and the expectations of master’s level learning.

Support is built into the course throughout your studies. Teaching is designed to be clear, structured and applied to real problems. You will learn through guided practical work, lab activities, case studies, technical tasks and project-based learning. This helps you build your knowledge step by step and develop confidence in both your technical and academic abilities. Skills such as critical thinking, problem solving, academic writing, communication and independent learning are developed within the modules themselves, as part of your normal learning experience.

Assessment is also designed to support your progress. In the early stages of modules, you will receive formative guidance and developmental feedback to help you understand what is expected and where you can improve. This helps you build confidence before completing larger or more complex assessments later in the course. As you progress, you will be better prepared to apply your knowledge in more independent and advanced work.

The course also supports your professional development. Through Research Methods and Professionalism, and through applied cybersecurity and AI activities across the course, you will develop awareness of professional practice, ethical issues and industry expectations. This helps you connect your academic learning with future career goals in cyber security, AI and related areas.

Your feedback is important to us. It helps us review and improve learning, teaching and support so that the course remains inclusive, relevant and responsive to student needs.

Currency:

Our MSc Cyber Security and Artificial Intelligence course is designed to remain current in a fast-changing field by combining strong academic foundations with content that is regularly reviewed and updated to reflect developments in research, technology and professional practice. The course covers core principles in cyber security and artificial intelligence that remain valuable over time, while also engaging with contemporary topics such as ethical hacking, machine learning, generative AI for cybersecurity, secure infrastructure, and incident management and response. This helps ensure that students develop knowledge and skills that are both academically rigorous and professionally relevant.

The course is further strengthened by the fact that the University’s computing courses are accredited by the BCS, the Chartered Institute for IT. This provides an important external benchmark for academic quality, professional relevance and curriculum standards. The course has also been designed with awareness of current developments in cyber security, artificial intelligence and the wider digital economy, helping to ensure that it remains relevant to emerging technologies and professional practice.

You are regularly encouraged to engage with research throughout the course. You will encounter current ideas, debates and developments in cyber security and AI, including research-informed teaching and, where appropriate, examples linked to staff expertise at the University. As you progress, you will develop your own enquiry, analysis and critical thinking skills through applied tasks, research activities and independent project work.

The course also prepares you to think creatively and critically about real-world challenges, including those linked to sustainability, innovation, enterprise and social responsibility. The University’s Graduate Attributes are embedded throughout the curriculum, helping students develop as knowledgeable learners, digitally fluent graduates, reflective professionals and responsible global citizens. By combining academic study, professional relevance and interdisciplinary thinking, the course supports you to become an adaptable, future-ready graduate who is well prepared for continued learning and a wide range of careers in cyber security, artificial intelligence and related digital fields.

Personalisation Opportunities:

Our MSc Cyber Security and Artificial Intelligence course provides you opportunities to shape your learning around your own interests, career plans and previous experience. While the course provides a strong foundation in core areas of cyber security, artificial intelligence, you will also have opportunities to explore topics and applications that matter to you. This helps make your learning more relevant, engaging and connected to your future goals. Across the course, many learning activities, case studies and assessments allow you to work on different problem areas and technical themes. This means you may be able to focus your work on areas that match your interests, such as secure infrastructure, AI for security, ethical hacking, threat analysis, automation for cyber security, or incident management and response. The dissertation gives you the greatest opportunity to personalise your learning, as you will investigate a specialist topic in depth and develop a project aligned to your own ambitions and strengths. The course also supports you in making informed choices about the direction of your learning. Guidance from module tutors will help you connect your interests with assessment topics, project ideas and longer-term career aims. Through Research Methods and Professionalism, as well as applied work across the course, you will be encouraged to reflect on your developing skills and professional interests so that you can build a pathway that is meaningful to you. Learning is designed to be relevant to a diverse student body. Real-world examples, technical tasks and discussions are intended to connect cyber security and AI to different industries, communities and practical challenges. You are encouraged to draw on your own experiences and perspectives as part of your learning. This helps make the course more meaningful and supports you in developing into a confident and capable postgraduate professional in cyber security and AI.

Employability in the Curriculum/Employability and Professional Development:

Our MSc Cyber Security and Artificial Intelligence course is designed to help you prepare for a wide range of careers in cyber security, artificial intelligence and related digital fields. Professional development is embedded throughout the course so that you can connect your academic learning with future career goals from the start of your studies. Through applied learning, technical projects and professional practice, you will develop a clearer understanding of how knowledge and skills in cyber security and AI are used in real organisational and industry contexts.

The course helps you build both technical and transferable skills. Across the modules, you will strengthen your abilities in problem solving, critical thinking, communication, independent learning and the professional use of digital tools and technologies. You will also engage with realistic technical tasks and project-based work that reflect the kinds of challenges found in cyber security and AI roles. This helps you gain relevant experience and build confidence in applying your skills in professional settings.

Research Methods and Professionalism module plays an important role in supporting your professional development. It helps you understand research, ethics, planning, professional responsibility and the standards expected in postgraduate and professional work. Across the course, you will also be encouraged to reflect on your strengths, respond to feedback and consider how your developing interests and specialist skills connect to your future goals.

Many learning activities and assessments are designed to reflect real-world practice. These may include technical reports, applied analysis, case study work, project tasks and presentations. Such activities help you develop not only subject knowledge, but also the confidence to explain your ideas, justify your decisions and present your work in a professional way. In this way, the course supports you not only to gain a qualification, but also to develop as a confident, capable and career-ready postgraduate graduate.