Programme Specification

UNIVERSITY OF WESTMINSTER

Course record information

Name and level of final award	• Bachelor of Science with Honours - Cyber Security and Forensics • Bachelor of Science with Honours - Cyber Security and Forensics with Industrial Experience • Bachelor of Science with Honours - Cyber Security and Forensics with International Experience The award is Bologna FQ-EHEA first cycle degree or diploma compatible
Name and level of intermediate awards	• Bachelor of Science (BSc) - Cyber Security and Forensics • Diploma of Higher Education (Dip HE) - Cyber Security and Forensics • Certificate of Higher Education (CertHE) - Cyber Security and Forensics
Awarding body/institution	University of Westminster
Teaching institution	University of Westminster
Status of awarding body/institution	Recognised Body
Location of delivery	Primary: Central London
Language of delivery and assessment	English
QAA subject benchmarking group(s)	Computing
Professional statutory or regulatory body	British Computer Society (BCS) (Pending: Please refer to Page 12 for further information)
Westminster course title, mode of attendance and standard length	• Cyber Security and Forensics BSc, Full-time, September start - 3 years standard length with an optional year abroad or placement
Valid for cohorts	From 2026/7 Level 4 entrants from 2026-7

Admissions requirements

There are standard minimum entry requirements for all undergraduate courses. Students are advised to check the standard requirements for the most up-to-date information. For most courses a decision will be made on the basis of your application form alone. However, for some courses the selection process may include an interview to demonstrate your strengths in addition to any formal entry requirements. More information can be found here: https://www.westminster.ac.uk/study/undergraduate/how-to-apply

Recognition of Prior Learning

Applicants with prior certificated or experiential learning at the same level of the qualification for which they wish to apply are advised to visit the following page for further information:

https://www.westminster.ac.uk/current-students/guides-and-policies/student-matters/recognition-of-prior-learning

Aims of the programme

Cyber security and digital forensics are rapidly evolving fields that play a critical role in protecting organisations, governments and individuals. This programme prepares you to meet the growing demand for skilled professionals who can detect, analyse and respond to cyber threats, and investigate incidents effectively. The course is aligned with the National Cyber Security Centre (NCSC) knowledge areas, including Strategic and Cultural Foundation, Risk and Threat Management, Technical and Operational Security, and Guidance and Principles.

You develop the knowledge, technical skills and professional behaviours needed to design secure systems, analyse vulnerabilities, respond confidently to cyber incidents and conduct digital investigations. You will learn to use both offensive and defensive tools, evaluate risks, identify weaknesses and recommend solutions that strengthen cyber resilience. As the discipline is fast-moving, you are encouraged to think creatively, consider global and societal impacts, recognise diverse viewpoints and design solutions that are fair, accessible and responsible.

The programme provides an inclusive and supportive learning environment that develops your communication, collaboration and problem-solving skills. Through practical work, group activities and project-based learning, you build the confidence and adaptability required to work effectively in a diverse professional cyber security environment. Sustainability is also embedded, helping you understand the environmental impact of technology and the importance of secure, energy-efficient systems.

The programme aims to:

- Equip you with a solid understanding of the fundamentals of cyber security, computer networks, digital forensics and relevant areas of computer science;
- Develop your theoretical and practical knowledge of the technologies underpinning cyber security, and enable you to apply this through laboratory work, simulations and real-world scenarios;
- Provide you with awareness of the socio-economic, ethical and legal considerations that shape cyber security practice;
- Encourage you to respond confidently to cyber incidents and to apply digital forensic techniques using the analytical and practical skills gained throughout the course;
- Provide an environment that enables you to collaborate and develop transferable skills such as project management, risk management, teamwork, leadership, entrepreneurship and effective communication;
- Ensure the course remains industry-focused and relevant through the use of current professional tools, practices and extracurricular engagement;
- Support the development of broader professional skills and behaviours, including communication, reflective practice and inclusive, respectful collaboration;
- Offer an engaging and rewarding learning experience that prepares you for professional careers in cyber security and digital forensics.

Employment and further study opportunities

University of Westminster graduates will be able to demonstrate the following five Graduate Attributes:

- Critical and creative thinkers
- Literate and effective communicator
- Entrepreneurial
- Global in outlook and engaged in communities
- Social, ethically and environmentally aware

University of Westminster courses capitalise on the benefits that London as a global city and as a major creative, intellectual and technology hub has to offer for the learning environment and experience of our students.

Employability is a central focus of the BSc Cyber Security and Forensics course. From your first year onwards, you receive support through workshops, events and guidance from the Careers Development Centre and the course team to help you develop your career plans, improve your CV and prepare for interviews and placement applications.

The course develops both your technical expertise and broader transferable skills, including teamwork, communication, critical thinking, report writing and problem-solving. At Level 4, core modules give you a strong foundation in programming, networks, cyber security, digital forensics and computer science. At Levels 5 and 6, you build specialist knowledge in areas such as offensive and defensive security, information governance, risk management and digital forensics. Optional modules allow you to broaden or deepen your expertise.

Work-based learning is embedded within the Level 5 module *Risk Management and IT Governance*, where you work on an industry-informed live project to apply theory in practice and develop skills such as project management, costing, risk assessment and written and oral communication. Other modules use realistic cyber scenarios such as penetration testing, incident response and forensic investigations to prepare you for professional environments.

After completing your second year you also have the option to take a year in industry, where you apply your knowledge directly in a professional environment, or an International Experience Year, which allows you to study or work abroad and develop global awareness, intercultural competence, and independence. The Careers Development Centre and the course team support you in finding and securing both types of placements, offering guidance on applications, CV preparation, and employer engagement.

Graduates are well suited to a wide range of cyber security and digital forensics roles, including:

Offensive Security

Penetration Tester / Ethical Hacker – Carries out controlled attacks to identify vulnerabilities in systems, applications and networks.
Vulnerability Assessor – Analyses systems for weaknesses and recommends practical mitigation measures.

Defensive Security & Operations

Security Operations Specialist – Monitors, configures and maintains security systems to protect an organisation’s infrastructure.
Security Software Developer / Architect – Designs and builds secure software and architectures with security integrated throughout the development lifecycle.
DevSecOps Engineer – Embeds automated security testing and monitoring into development and operations processes to ensure resilient deployments.

Digital Forensics & Incident Response (DFIR)

Incident Responder – Detects, investigates and contains security breaches, restoring systems and reducing operational impact.
Digital Forensics Analyst – Collects and examines digital evidence using specialist tools to support investigations and legal or organisational processes.

Governance, Risk & Assurance

Information Security Auditor / Risk Manager – Evaluates organisational risk, checks compliance with regulations and standards, and recommends controls to strengthen security posture.

You may also choose to continue your studies at Master’s or Doctoral level, and the course team will support you in exploring further study opportunities.

What will you be expected to achieve?

Learning outcomes are statements of what successful students have achieved as a result of learning. These are threshold statements of achievement the learning outcomes broadly fall into four categories:

- The overall knowledge and understanding you will gain from your course (KU)
- Graduate attributes are characteristics that you will have developed during the duration of your course (GA)
- Professional and personal practice learning outcomes are specific skills that you will be expected to have gained on successful completion of the course (PPP)
- Key transferable skills that you will be expected to have gained on successful completion of the course. (KTS)
- Cognitive Skills, are learning outcomes that help build a conceptual understanding that is necessary to devise and sustain arguments, and/or to solve problems and comment on research.

Level 4 course learning outcomes: upon completion of Level 4 you will be able to:

- LO4.1 Demonstrate knowledge and understanding of the core principles and the fundamental concepts of computer science. (KU)
- LO4.2 Explain the fundamentals of cybersecurity and digital forensics, focusing on how networking, hardware, and data contribute to secure systems. (KU GA KTS CS)
- LO4.3 Demonstrate a good understanding of a range of underlying mathematics theories related to computer science and cyber security. (KU CS)
- LO4.4 Design and implement simple programs and digital solutions, using appropriate programming languages, development tools, and structured testing approaches. (GA KTS SS CS)
- LO4.5 Demonstrate a knowledge and understanding of current technology and trending future technology in computer systems, cybersecurity, design tools and techniques as taught. (KU GA PPP KTS)
- LO4.6 Gather and assimilate information, with some guidance, and apply it appropriately and then communicate technical information succinctly and accurately, by means of presentations, written reports, appropriate diagrams, and discussion (GA PPP KTS)
- LO4.7 Plan and coordinate work required for structured group tasks, keeping to set deadlines given direction and guidance. (GA PPP KTS)
- LO4.8 Recognise and apply professional codes of conduct and ethical and sustainable principles, demonstrating awareness of equality, diversity and inclusion when engaging in the computing practice. (KU GA PPP)

Level 5 course learning outcomes: upon completion of Level 5 you will be able to:

- LO5.1 Analyse and apply cryptographic techniques to secure data and communications, evaluating their effectiveness and limitations in practical cybersecurity contexts. (KU GA PPP SS CS)
- LO5.2 Analyse and evaluate risk reduction strategies, adopting a holistic approach that applies appropriate risk management principles in line with relevant standards and legislation. (KU GA PPP SS CS)
- LO5.3 Critically investigate complex digital forensic cases using practical tools, skills, methodologies and practices to identify computer crime and cyber incidents. (KU GA PPP SS CS)
- LO5.4 Concisely and accurately document findings in a clear and structured format suitable for both technical and non-technical audiences, demonstrating awareness of professional and legal standards. (GA PPP KTS)
- LO5.5 Evaluate and compare sustainable security control solutions and algorithms for securing complex organisational networks, assessing their effectiveness, limitations, and potential societal and environmental impacts. (KU GA PPP CS)
- LO5.6 Analyse and evaluate security vulnerabilities in web and networked systems by conducting structured penetration testing, interpreting findings, and recommending appropriate mitigation strategies. (KU GA PPP SS CS)
- LO5.7 Work effectively either in a group or individually and be able to recognise development needs for the acquisition of new skills. (GA PPP KTS)
- LO5.8 Apply and integrate academic knowledge and professional skills in a real-world context, analysing project outcomes and reflecting on personal and professional development within the workplace. (GA PPP KTS SS CS)
- LO5.9 Adopt an inclusive approach to engineering practice and recognise the responsibilities, benefits and

importance of supporting equality, diversity and inclusion. (GA PPP)

Additional Year course learning outcomes: upon completion of Additional Year you will be able to:

- IEY.1 Enable personal development by devising a programme of international study that complements the content of the home degree programme and/or develops other interests. (GA PPP KTS)
- IEY.2 Appreciate the challenges and opportunities of studying/ working in an international context. (GA PPP KTS)
- IEY.3 Demonstrate an understanding of, and respect for, the cultural norms and differences of the host country at a societal level as part of an inclusive, global outlook. (GA PPP KTS)
- IPY.1 Experience commercial application of engineering knowhow and identify the factors affecting products and services in IT industry. (KU GA PPP KTS)
- IPY.2 Demonstrate the acquisition of a range of professional, practical, and key-transferrable skills relevant to the fields of computing (KU GA PPP KTS)
- IPY.3 Take personal responsibility for directing your own learning and future career making the best use of the opportunities, experiences and people that were available to you during your placement year. (GA PPP KTS)
- IPY.4 Draw upon the diverse approaches, perspectives, knowledge and experience of a diverse workforce, treating all individuals with respect and recognising their contribution to the host organisation. (KU GA PPP KTS)

Level 6 course learning outcomes: upon completion of Level 6 you will be able to:

- LO6.1 Critically evaluate, design, and implement security measures on different technologies and evaluate their effectiveness against known attacks. (GA PPP SS CS)
- LO6.2 Select and apply advanced methods, principles, and concepts to identify cyber incidents and be able to forensically investigate, make decisions in complex and unpredictable contexts and interpret and analyse results obtained in a systematic manner. (KU GA PPP SS)
- LO6.3 Independently gather, assimilate, and critically evaluate information to a given cyber security or digital forensics issue, choose and formulate cost and effectiveness of a given set of solutions, and select and implement the most viable solution (KU GA KTS CS)
- LO6.4 Critically evaluate emerging cyber threats and countermeasures, including the role of artificial intelligence in both offensive and defensive contexts, to propose informed and ethical approaches to enhancing cybersecurity resilience. (KU GA CS)
- LO6.5 Critically evaluate and apply advanced defensive and offensive security methodologies to design, assess, and justify effective strategies for protecting and testing complex systems. (GA PPP SS CS)
- LO6.6 Select, analyse, and communicate complex technical information succinctly and accurately to expert and non-expert audiences, reviewing its reliability, validity, and significance by means of presentations, written reports, and discussion. (GA PPP KTS CS)
- LO6.7 Undertake research tasks with minimum guidance and critically evaluate arguments, assumptions, and abstract concepts. Organise and present information concisely and correctly and manage project work, adhering to given timetables and targets (GA PPP KTS CS)
- LO6.8 Recognise and assess risk limitations pertaining to a given problem including those related to the environment, sustainability, society, health and safety and regulation and suggest ways to mitigate this risk. (GA PPP KTS)
- LO6.9 Practice life-long learning and entrepreneurial skills using independent and creative thought through the gathering and assimilation of information gained through practical work using logbooks, minutes of meetings, social media sites and other novel methods. (GA PPP KTS)

How will you learn?

Learning methods

The BSc Cyber Security and Forensics course uses a variety of teaching and assessment methods to ensure that you are supported to achieve your full potential and the best possible outcome. A principal aim of the course is to prepare you for professional practice or further study in cyber security and forensics. To this end, the course is organised into a structured set of modules at different levels, each directly aligned with the aims and learning outcomes of the programme. These modules provide the main learning opportunities across the course. Every module consists of learning activities delivered over several weeks, designed to help you develop the knowledge and skills required in cyber security and

forensics.

A key principle that underpins the learning and teaching methods on this course is learning through practice. To understand and master the specialist skills and techniques required in cyber security and forensics, you learn by doing. This applies to practical cyber security and forensics development tasks through project work, as well as analytical and problem-solving skills through the application of taught principles to technical challenges.

Much of your learning takes place through active participation in interactive practical sessions. At the end of these sessions, you receive feedback to help you understand your progress. For example, laboratory activities often form part of the formative assessment process, where you are supported to complete tasks and receive written, verbal, or qualitative feedback. These formative activities build your confidence and capability so that you are well prepared for the final summative assessments in each module. Throughout the course, lecturers provide feedback individually or to the whole class.

To develop transferable and professional skills, you take part in a range of activities such as group work, code reviews, presentations and collaborative problem-solving tasks. These experiences help you build teamwork, communication and time-management skills. You will also be required to present and defend your work, which enables you to reflect critically on your learning and develop the ability to communicate your ideas clearly and concisely.

How is Equality, Diversity, and Inclusivity (EDI) addressed in your course

Equality, Diversity and Inclusivity are embedded throughout the programme. You learn in an environment that is supportive, respectful and accessible, with teaching methods and learning resources designed to meet a wide range of needs and backgrounds. You are encouraged to work in ways that reflect your interests, strengths and career ambitions, and you will have opportunities to shape your learning through your project choices and optional modules.

You study in a community built on mutual trust and respect, where collaboration and open discussion are central to the learning experience. Teaching materials are designed to be as inclusive as possible, and staff work with you to identify and remove barriers to learning. A range of assessment types is used across the course to give you different ways to demonstrate your abilities.

You benefit from an inclusive physical and digital learning environment, access to specialist support where required, and exposure to a diverse set of perspectives through guest speakers, group work and extracurricular activities such as game jams. The course team is committed to ensuring that you can participate fully, develop confidence, and succeed in a diverse and changing industry.

Sustainability

This programme aligns with the University's commitment to the UN Sustainable Development Goals and the *Being Westminster* values by embedding sustainability thinking across all levels of study. You will be encouraged to consider the environmental and economic impacts of technology and practice as part of your learning, with each level of the course integrating domain-relevant sustainability principles. This ensures that, as you progress, you develop both the technical expertise and the responsible mindset expected of modern computing and engineering professionals.

Teaching methods

We use a range of teaching methods to support your learning. Our aim is to prepare you for professional practice by exposing you to industry-relevant tools, techniques and development environments throughout the course.

You learn through lectures, practical laboratory sessions, workshops, project work, individual supervision and guided online materials. Lectures introduce fundamental concepts, methods and development strategies, and help you understand how different areas of cyber security and forensics connect. These sessions include interactive elements to encourage active engagement.

Practical laboratory sessions give you hands-on experience with cyber security tools, forensic techniques and investigative problem-solving. You will configure and secure systems, analyse logs and network traffic, examine digital evidence, and carry out controlled offensive and defensive tasks in safe, supervised environments. Collaborative exercises allow you to apply concepts from lectures to realistic scenarios such as incident response, threat analysis and vulnerability assessment. Workshops focus on developing professional skills such as documenting investigations, producing technical reports, interpreting legal and regulatory requirements, and working towards key project milestones.

Some modules use online quizzes and other activities to support remote learning. These quizzes provide immediate feedback, help you monitor your understanding and allow tutors to identify areas where additional support may be needed.

Authentic assessment is embedded across the course so that you practise skills required in the cyber security

profession. You will work on investigative tasks, applied technical problems and project-based assignments where you create artefacts that reflect real cyber security contexts.

Your final-year project brings together the knowledge and skills gained across the programme. You will design and deliver a substantial piece of work, supported by an academic supervisor who guides you through the process.

To ensure accessibility and flexibility, each module provides online support such as access to learning materials, reading lists, discussion spaces and virtual study rooms. You also receive academic support from module leaders, your personal tutor and the course team at key decision points, such as selecting option modules or choosing your final-year project.

Independent study is an essential part of the course. We help you develop the habits and skills needed for continual professional development (CPD) through group-based activities, taught frameworks, extracurricular opportunities and assessment formats that encourage planning, reflection and self-directed learning.

Assessment methods

Assessment and feedback are central to your learning. They help you understand your progress, reflect on what you have achieved, identify areas for improvement and make informed decisions about your independent study. Assessment on the BSc Cyber Security and Forensics course is guided by the principles of Purpose, Progression and Personalisation.

Purpose

Assessments are designed to be authentic, giving you opportunities to apply your computing knowledge and professional skills to real-world problems using industry-relevant tools and techniques. Each assessment method is clearly aligned with the module learning outcomes, and the workload is balanced so that you can manage your time effectively across the course.

Progression

Assessments are structured to support your development over time. You encounter a variety of assessment types that encourage new learning rather than unnecessary repetition. Less familiar formats are introduced gradually, supported by formative activities such as practice labs, workshops, or targeted exercises that help you prepare for summative tasks.

Personalisation

You are encouraged to make assessments your own through your design choices, implementation approaches and reflective work. You receive timely feedback on all assessments, with clear guidance on how to improve your performance in future tasks.

Across the programme, assessment is designed to be:

- demonstrative, allowing you to test and consolidate your understanding;
- rigorous, requiring correct, efficient and well-reasoned solutions;
- challenging, encouraging deep analysis and problem-solving;
- workplace relevant, reflecting the expectations and practices of the computing profession.

You complete a range of assessment types, from small technical tasks carried out in practical sessions to larger individual and group projects developed over a full semester. Some assessments require independent work, while others involve teamwork that mirrors professional cyber security environments.

Each module includes formative assessment, which does not count toward your final grade but helps you identify your strengths, diagnose gaps in your understanding and receive feedback that guides your progress. Formative activities may include quizzes, short tests, reflective tasks or group-based problem-solving exercises. Summative assessments contribute to your module grade and are always assessed against clear criteria linked directly to the module learning outcomes.

The course provides inclusive, engaging and authentic assessment and feedback strategies designed to give you equal opportunities to demonstrate your abilities and to support your development as a competent and confident cyber security professional.

Examples of Summative assessments used in the course

Practical Coursework / Practical based portfolio	You will be expected to complete lab tasks following lab guidelines and either answer specific questions about the labs (Coursework) or analyse your results based on a given scenario (Portfolio).
Group Presentation with/without Group Coursework	You will be working in a group, typically of 3 to 4 members, investigating a specific problem, or research a specific topic. You will be expected to give a presentation to demonstrate your group work. This is usually followed by a brief discussion and questions and answers with your peers and instructor. Generally, you will need to discuss in detail what the group has achieved, and how, and also how the work and the team member responsibilities were distributed.
ICT (exam conditions)	You will be expected to sit an in-class test under timed conditions. Typically, these in-class tests can be a closed-book or open-book where you will have access to certain materials. This type of assessment is used to assess your understanding of the fundamentals, theory, and paradigms. Tests help ensure you can demonstrate that you have developed a deep understanding of the subject which enables you to cope with complex problems that require deep inside in order to provide secure and optimal solutions. This time-constrained assessment is authentic in that it verifies that you will have sufficient depth and coverage of knowledge in order to successfully solve typical time-critical cyber security problems. It also helps you prepare for other professional exams and training.
Lab-based practical	You will be expected to complete a specific lab task in the lab. This will be in most cases a timed activity where you are given instructions and a set of tasks to complete.
Coursework Case study	You will be required to work on a scenario that illustrates a specific problem. You will have to study this problem and assess it and take decisions or make recommendations. This will require research and analysis and potentially implementation in order for you to produce an assessment and recommendation. This type of assessment is used to assess your understanding of topics related to your module and how you can apply your knowledge to a given scenario.
Research essay	You will be expected to conduct in-depth research on a specific topic. This involves examining various resources, concepts and ideas about the topic you are researching.
Oral Assessment and/or Individual Presentation	You will be expected to present in a form of either a presentation or discussion on a given topic. This could also be a part of your dissertation where you will be expected to sit a viva voce assessment to defend your work.
Artefact	You will be expected to produce a product such as code implementation or a document containing a set of recommendation and guidelines that demonstrate your ability to innovate to provide solutions to a given problem.
Report	You will be expected to produce a document that outlines activities you have undertaken. This can be either for lab work that you have completed, a work experience and work placement that you undertook or your reflective comments about a specific topic.

Dissertation	This will be the biggest document you will have to produce for your entire studies. You will be expected to produce an extended piece of written work, that contains substantial evidence of research, investigations, and possibly implementation, all related to a specific problem you have chosen. Dissertations are the result of your independent work, carried out under the guidance of a supervisor.

Graduate Attribute	Evident in Course Outcomes
Critical and creative thinker	IPY.1, IPY.3, LO4.1, LO4.2, LO4.3, LO4.4, LO5.1, LO5.2, LO5.3, LO5.5, LO5.6, LO5.8, LO6.1, LO6.2, LO6.3, LO6.4, LO6.5, LO6.6, LO6.7, LO6.9
Literate and effective communicator	IEY.1, LO4.6, LO4.7, LO5.4, LO6.3, LO6.6, LO6.7, LO6.9
Entrepreneurial	IPY.1, IPY.2, IPY.3, LO4.5, LO6.9
Global in outlook and engaged in communities	IEY.1, IEY.2, IEY.3, IPY.4, LO4.5, LO4.8, LO5.2, LO5.4, LO5.8, LO5.9, LO6.6, LO6.8, LO6.9
Socially, ethically and environmentally aware	IEY.2, IEY.3, IPY.4, LO4.2, LO4.8, LO5.1, LO5.2, LO5.3, LO5.4, LO5.5, LO5.6, LO5.7, LO5.8, LO5.9, LO6.1, LO6.2, LO6.3, LO6.4, LO6.5, LO6.6, LO6.7, LO6.8, LO6.9

Course Structure

This section shows the core and option modules available as part of the course and their credit value. Full-time Undergraduate students study 120 credits per year. Course structures can be subject to change each academic year following feedback from a variety of sources.

Modules are described as:

- **Core** modules are compulsory and must be undertaken by all students on the course.
- **Option** modules give you a choice of modules and are normally related to your subject area.
- **Electives**: are modules from across the either the whole University or your College. Such modules allow you to broaden your academic experience. For example, where electives are indicated, you may choose to commence the study of a foreign language alongside your course modules (and take this through to the final year), thereby adding further value to your degree.
- Additional information may also be included above each level, for example, where you must choose one of two specific modules.

Modules

Level 4

Module Code	Module Title	Status	UK credit	ECTS
4ELEN010W	Applied Mathematics	Core	20	10
4COSC003W	Foundations of Professional Computing	Core	20	10
4CSEF001W	Introduction to Cyber Security and Digital Forensics	Core	20	10
4NTCM002W	Introduction to Networks	Core	20	10
4CSEF002W	Programming for Cyber Security and Digital Forensics	Core	20	10
4COSC011W	Web Design and Development	Core	20	10

Level 5

Module Code	Module Title	Status	UK credit	ECTS
5NTCM006W	Applied Cryptography	Core	20	10

Module Code	Module Title	Status	UK credit	ECTS
5CSEF001W	Digital Forensics	Core	20	10
5CSEF002W	Network Penetration Testing	Core	20	10
5CSEF003W	Risk Management and IT Governance (WBL)	Core	20	10
5CSEF004W	Web Application Penetration Testing	Core	20	10
5DATA006W	Data Visualisation and Communication	Option	20	10
5COSC025W	Human Computer Interaction and User Experience	Option	20	10
5ELEN016W	Operating Systems	Option	20	10
		Elective	20	10

Additional Year

Students who undertake the 4 year course must pass module 5COSC028W to achieve the award "with Industrial Experience" or pass module 5COSC027W to achieve the award "with International Experience" .

Module Code	Module Title	Status	UK credit	ECTS
5COSC028W	Computer Science and Engineering Industrial Placement	Option	120	60
5COSC027W	Computer Science and Engineering International Year	Option	120	60

Level 6

Module Code	Module Title	Status	UK credit	ECTS
6CSEF002W	Cyber Security and Forensics Final Project	Core	40	20
6CSEF004W	Incident Response and Malware Analysis	Core	20	10
6CSEF005W	Wireless Networks Security	Core	20	10
6CSEF006W	Advanced Penetration Testing	Option	20	10
6CSEF007W	AI in Cyber Security	Option	20	10
6CSEF001W	Cyber Security Threats and Counter Measures	Option	20	10
6CSEF003W	Defensive Programming Techniques	Option	20	10

Please note: Not all option modules will necessarily be offered in any one year. In addition, timetabling and limited spaces may mean you cannot register for your first choice of option modules.

Professional body accreditation or other external references

The course has been designed with reference to:

- QAA Subject Benchmark for Computing
- Engineering Council Accreditation of Higher Education Programmes (AHEP), fourth edition
- QAA Guidelines for Preparing Programme Specifications
- SEEC Credit Level Descriptors for Further and Higher Education

The British Computer Society (BCS) professional accreditation ensures independent validation that the course meets high standards set by the profession. It also benchmarks the course against those of other institutions both nationally and internationally and supports the continued improvement of the course, highlighting areas of best practice across institutions. For you as a student being on an accredited course provides a pathway to professional registrations such as Chartered IT Professional (CITP), Chartered or Incorporated Engineer (CEng/IEng) and Registered IT Technician (RITTech).

BSc Cyber Security and Forensics is intended to fulfil the educational requirements of BCS for the CITP and partial CEng. Due to the 5-year accreditation timeline the course will be considered for the accreditation in 2027. The accreditation will be backdated to include the first intake from September 2023. On successful completion of this process your course will become accredited in 2027.

Course management

BSc Cyber Security and Forensics course is under the School of Computer Science and Engineering and the management structure supporting the course is as follows:

- the Course Leader is responsible for day to day running and overall management of the course and development of the curriculum.
- the Head of School holds academic responsibility for the course and other courses within the School.
- the Head of the College of Design, Creative and Digital Industries, holds overall responsibility for the course, and for the other courses run by the College.

Academic regulations

The current Handbook of Academic Regulations is available at westminster.ac.uk/academic-regulations.

Course specific regulations apply to some courses.

Academic Support

Upon arrival, an induction programme will introduce you to the staff responsible for the course, the campus on which you will be studying, the Library and IT facilities and additional support available. You will be provided with a Course Handbook, which provides detailed information about the course. Each course has a course leader or equivalent. All students enrolled on a full-time course and part-time students registered for more than 60 credits a year have a personal tutor, who provides advice and guidance on academic matters. The University utilises a Virtual Learning Environment called Blackboard, where students access their course materials and can communicate and collaborate with staff and other students. Further information on Blackboard can be found at https://www.westminster.ac.uk/current-students/studies/your-student-journey/when-you-arrive/blackboard

The Academic Learning Development Centre supports students in developing the skills required for higher education. In addition to online resources in Blackboard, students can also attend Study Skills workshops and schedule one-to-one appointments. Further information on the Academic Learning Development Centre can be found at westminster.ac.uk/academic-learning-development.

Learning support includes our libraries, each of which holds a collection of resources related to the subjects taught at that site. Students can search the entire library collection online through the Library Search service to find and reserve printed books, and access electronic resources (databases, e-journals, e-books). Students can choose to study in the libraries, which have areas for silent and group study, desktop computers, laptops for loan, photocopying and printing services.

Support Services

The University of Westminster's Student and Academic Services department provides a range of advice and guidance.

Further information on the advice available to students can be found at https://www.westminster.ac.uk/student-advice

The University of Westminster Students' Union also provides a range of facilities to support students during their time at the University. Further information on UWSU can be found at https://www.westminster.ac.uk/students-union

How do we ensure the quality of our courses and continuous improvement?

The course was initially approved by a University Validation Panel. University Panels normally include internal peers from the University, academic(s) from another university, a representative from industry and a Student Advisor.

The course is also monitored annually by the College to ensure it is running effectively and that any issues that might affect the student experience have been appropriately addressed. Staff will consider evidence from various sources, including student surveys, student progression and achievement, and reports from external examiners, to evaluate the effectiveness of the course and make necessary changes.

Periodic reviews are also conducted to ensure that the curriculum remains up-to-date and that the skills acquired on the course continue to be relevant to employers. Representative students meet with a panel to provide feedback on their experiences. Student feedback from previous years is also part of the evidence used to assess the course's performance.

How do we act on student feedback?

Student feedback is important to the University, and student views are taken seriously. Student feedback is collected in various ways.

- Through student engagement activities at the course and module level, students have the opportunity to express their voice in the running of their course. Course representatives are elected to expressly represent the views of their peers. The University and the Students' Union work together to provide a full induction to the role of the course representatives.
- There are also School Representatives appointed jointly by the University and the Students' Union who meet with senior School staff to discuss wider issues affecting student experience across the School. Student representatives are also represented on key College and University committees.;
- All students are invited to complete a questionnaire for each module. The feedback from this will inform the module leader on the effectiveness of the module and highlight areas that could be improved.
- Final-year undergraduate students will be asked to complete the National Student Survey, which helps inform the national university league tables. Postgraduate students will be asked to complete the Postgraduate Taught Survey (PTES).

This programme specification provides a concise summary of the main features of the course and the learning outcomes that a student may reasonably be expected to achieve and demonstrate if they take full advantage of the learning opportunities provided. This specification is supplemented by the Course Handbook, Module proforma and Module Handbooks provided to students.

Additional Details

When CS&E Industrial Placement Year is taken the award of BSc Cyber Security and Digital Forensics with Industria Experience is available. When CS&E International Study Year is taken the award of BSc Cyber Security and Digita Forensics with International Experience is available.