UNIVERSITY OF
LEADING
THE WAY
WESTMINSTER

PROGRAMME SPECIFICATION

Course record information

Name and level of final award:	MSc The *MSc in Cyber Security and Forensics* an MSc degree that is Bologna FQ-EHEA second cycle degree or diploma compatible.
Name and level of intermediate awards:	Postgraduate Diploma Postgraduate Certificate
Awarding body/institution:	University of Westminster
Status of awarding body/institution:	Recognised Body
Location of delivery:	Cavendish Campus, London, United Kingdom
Language of delivery and assessment:	English
Course/programme leader:	Paul Douglas
Course URL:	www.westminster.ac.uk/courses/subjects/computer-science-and-software-engineering/postgraduate-courses
Mode and length of study:	Full Time – 1 year Part-Time (Evening / Mixed) – 2 years minimum
University of Westminster course code:	W50
JACS code:	
UCAS code:	P034084 (FT & Part-Evening)
QAA subject benchmarking group:	Subject Benchmark Statement: Master's degrees in Computing, 2011, available online www.qaa.ac.uk/en/Publications/Documents/SBS-Masters-degree-computing.pdf
Professional body accreditation:	British Computer Society (BCS) TBC in Nov 2016
Date of course validation/review:	May 2016
Date of programme specification:	May 2016

Admissions requirements

The course builds on students' graduate competences and develops further their logical, analytical skills and technical skills in a way that they can be applied to Security and Forensics problems. Consideration will be given to all applicants with a good Honours (normally 2.ii or above) degree from a British University or overseas equivalent in an IT/Computing discipline or another discipline that either provides important underpinning for / insight into IT/Computing.

The department is committed to widening participation in education, particularly with respect to mature applicants whose extensive experience of working in business and industry has given them maturity that may outweigh any gaps in academic qualifications. Applications of such candidates are encouraged, and will be considered carefully; moreover, where maturity may outweigh formal academic qualifications, the academic qualification requirement will be relaxed. Due to the technical nature of the course, applicants whose first degree discipline is not in Computing, Science or Engineering and do not have a strong Computing flavour will be considered only if they can demonstrate that they have sufficient, in the admissions tutor's opinion, practical knowledge / work experience of computing to complete the course.

All applicants are required to show competence in both written and spoken English; thus, overseas applicants whose first language is not English are normally required to have attained the equivalent of an IELTS score of at least 6.5 with 6:0 or above in each element prior to joining the course (more information on minimum scores for other language tests can be obtained for the admissions office).

All applicants are required to submit with their application, copies of their academic and/or professional qualifications and transcripts, two references (one of which should be academic, for applicants who have been in Higher Education in the 5 years prior to applying for the course), and a statement explaining the reasons they want to be admitted to the course, what they expect from the course, how they are going to achieve it, what they will bring to the course, what their career aspirations are and how they think the course can help them achieve those aspirations.

The admissions policy conforms to the Equal Opportunities Policy and the Admissions Policy of the University of Westminster. Each application is considered on its individual merits and decisions in admitting applicants to the course are made based on evidence that the applicant is likely to benefit from the course and to complete it satisfactorily.

Occasionally, applicants may also be asked to attend an informal interview with the Admissions Tutor that aims at establishing applicants' suitability for the course. For applicants living locally, these interviews may have the form of an invitation to one of the University's postgraduate information events, where applicants can meet members of the course team and the Admissions Tutor, ask questions and discuss any issues regarding the course. Alternatively, for applicants living further afield such interviews may be contacted over the phone or by teleconferencing.

Successful applicants with disabilities are contacted by the University of Westminster's Disability Support Co-ordinator and are asked to make an appointment with the University's Disabilities Officer, in order for the student to assess the University's facilities for disabled students. Following that meeting if it is deemed necessary a further discussion with the Course Leader may be appropriate to enable the applicant to make an informed decision.

All successful applicants are sent well before the start of the course more detailed information about module, timetable and an up-to-date reference list of textbooks that they can use to prepare for the course. Successful applicants, who are not practitioners in the field and/or who feel that they may need to do more preparation before the start of the course, are strongly advised to contact the Admissions Tutor or the Course Leader for advice.

Part-time students are expected to be in full-time employment. Moreover, students are warned that a Master's programme of this type is by definition very intensive and it requires their total commitment if they are to be successful.

Aims of the course

The course has been designed with a high degree of relevance to industry's needs. By it is nature the course is practitioner oriented and it provides highly marketable Computer Security and Digital Forensics skills. The course is aimed at (a) graduates with a good Honours degree with a substantial Computing flavour who wish to pursue a postgraduate qualification in the field of Computer Security and Digital Forensics; and (b) practitioners who want to enhance their professional abilities, develop further their careers, update their technical skills and/or deepen their knowledge/understanding of state of the art and emerging technologies.

Overall the course aims to develop students' competences and equip them with specific technical skills so that they can either work effectively as IT security professionals who have a strong awareness of the environment in which they operate and/or be able to pursue research oriented academic study. More specifically, the course provides a balanced study that aims at producing graduates capable of:

AIM1: promoting public awareness of, and debate about, the social need for and technical challenge of digital security;

AIM2: utilising their problem solving skills and their knowledge of various techniques / tools / methods, to deliver solutions to Computer Security related problems;

AIM3: developing cyber security and forensics as an appropriate vehicle of postgraduate academic study;

AIM4: enabling students to develop as confident and reflective digital security practitioners, able to work independently and to a professional standard;

AIM5: participating in professional networking within a rapidly developing cyber security and forensics community;

AIM6: fostering research within the field of cyber security and forensics, and enable students to carry out further study and independent academic or practice-based research;

AIM7: developing professional attitudes as well as the interpersonal and entrepreneurial skills required of a practitioner in the industry;

AIM8: being self-motivated and independent learners, self-aware and able to reflect on their learning, and to manage their own personal development and career planning.

Employment and further study opportunities

Today's organisations need graduates with both good degrees and skills relevant to the workplace, i.e. employability skills. The University of Westminster is committed to developing employable graduates by ensuring that:

- career development skills are embedded in all courses;
- opportunities for part-time work, placements and work-related learning activities are widely available to students;
- staff continue to widen and strengthen the University's links with employers in all sectors, involving them in curriculum design and encouraging their participation in other aspects of the University's career education and guidance provision;
- staff are provided with up-to-date data on labour market trends and employers' requirements which will inform the service delivered to students.

Typically graduates of the course will seek employment as computer forensics professionals, typically working for large businesses (e.g. banks), law enforcement agencies and Government departments.

Employment

Recent graduates have joined a variety of organisations, including Barclays Bank, Deutsche Bank, the Metropolitan Police, City of London Police, Network Rail, MoD and several oversees police forces.

Further Studies

PhD in Digital Forensics at Cranfield University, PhD in Digital Security at University of Westminster.

Learning outcomes

Learning outcomes are statements on what successful students have achieved as the result of learning. These threshold statements of achievement and are linked to the knowledge, understanding and skills that a student will have gained on successfully completing a course.

Knowledge and understanding

Graduates of the course will:

KU1: have a systematic understanding and a critical awareness of current problems and/or new insights in the area of Cyber Security and Forensics, much of which is informed by academic research and professional practice in the particular field;

KU2: have a comprehensive understanding of the techniques and approaches applicable for the design, development, implementation and maintenance of computer security systems;

KU3: show originality and innovation in the application of knowledge and techniques for designing, developing, implementing and maintaining such systems;

KU4: show critical awareness of current research issues, problems and/or insights;

KU5: understand and be able to participate within the professional, legal and ethical framework as professionals in field;

KU6: evaluate the risk posed by cyber crime to our society;

KU7: develop and apply new security strategies and forensic analysis techniques.

Specific Skills

- identify, preserve and analyse sources of digital evidence;
- use and critically evaluate computer forensic software tools;
- present digital forensic evidence in a systematic manner in a court of law;
- devise and implement digital security policies;
- advise corporate clients on network security issues, evaluate current systems and suggest improvements where appropriate
- decision-making in complex and unpredictable situations; and
- the independent learning ability required for continuing professional development.

Key transferable skills

Upon completion of the course students will have developed a number of general rather than discipline-specific skills which any practitioner must have if s/he is to be successful. These key transferable skills developed and assessed at postgraduate level are:

KTS1: Group working
Students will be able to (a) work effectively within a group both as group leaders and/or group members; (b) clarify tasks and make appropriate use of group members abilities; (c) negotiate and handle conflict with confidence; and (d) participate effectively in the peer review process;

KTS2: Learning resources
Students will be able to use a full range of learning resources to carry out literature reviews and engage in research activity;

KTS3: Self-evaluation
Students will be able to reflect on own and others functioning; participate effectively in the peer review process and analyse and identify ways to improve practice; continue to advance their knowledge and understanding, and recognise their development needs and to develop new skills to a high level;

KTS4: Management of information
Students will be able to competently undertake research tasks with minimum guidance; sieve through information clatter to identify relevance, to organise and present information effectively using different media;

KTS5: Autonomy
Students will be independent and self-critical learner, who can act autonomously in planning and implementing tasks and who will be able to guide the learning of others;

KTS6: Communication
Students can engage confidently in academic and professional communication with others, reporting on action clearly, autonomously and competently;

KTS7: Problem solving
Students have independent learning ability required for continuing professional study, making professional use of others where appropriate.

Some of these skills, such as Problem Solving skills and Communication skills, are intrinsic to the nature of the course and thus they have been assessed / developed by each and every assessment component. For other skills, like group working, effort has been made to be included in as many modules as possible because ability to work effectively with/within a group, to clarify/allocate tasks, negotiate load and resolve conflict are important skills that IT professionals involved in IS design should have.

Learning, teaching and assessment methods

Learning & Teaching

The learning strategies employed on the course vary depending on the module and the learning outcomes for each module. The delivery of most of the modules involves teaching using traditional formal lectures and ‘structured lectures’, where lecturing is broken up by periods of student-led activity. The lectures are used to provide a firm grounding in the theory, methods and techniques relevant to the module’s topic. Lectures are usually supplemented by further instructor led sessions, where theoretical or practical in nature problems are addressed. During these sessions students will attend problem solving tutorials, sometimes working alone, often working in groups, sometimes working on paper, often working at a PC or workstation, always with a member of staff guiding the work or on hand to help resolve problems. To integrate the knowledge gained in individual modules common case studies, where possible, are used across modules, with each module tackling different aspects of the same problem. Modules with a highly technical and practical content are typically delivered in the form of workshops. These take place in the forensics lab and they combine material normally covered in a lecture with practical/hands-on exercises. In particular, the various concepts / constructs of the module's topics are introduced in short bursts and they are followed by a series of practical exercises that aim at enabling students to appreciate these concepts / constructs and understand how they can be used. This approach encourages students to actively participate in the development of a solution by allowing them to (a) express their thoughts; and (b) get immediate individual feedback from peers and/or the instructor. Finally, there are also seminar sessions in which students will present work to their classmates and assess each other's work.

The project is probably the most important aspect of the Master's programme. It plays a unifying role in the course by providing, in effect, the equivalent of a programme of integrated assignments which draws directly on all of the taught modules of the course. Students are expected to work on the project that is on a topic that each student has chosen, in the summer months after the end of the taught part of the course under the supervision of a member of academic staff. Generally, there are three types of projects: (a) projects proposed by students themselves (typically such projects are based on idea(s) a student has come up with that were developed following a supervisor input to an appropriate for the level and standard project); (b) projects based on an idea suggested by teaching staff that a student has researched and developed to an appropriate for the level and standard project; and finally (c) work-based projects, the latter of which, in most cases, are undertaken by part-time students.

To help students build the required background for their project and develop further their research skills, students are required to take a project preparatory module as part of which they are introduced to various project areas; choose the topic/area of their project; are allocated a project supervisor who, in most cases, has research interests in the area of a student's chosen project topic; research the area of their project; and devise a proposal detailed enough that will enable them to complete their project.

The supervisor acts in effect as someone who will guide students throughout the various phases of the project and who students will turn to in order to discuss their project work and receive feedback on the progress made and to have informed discussions on technical and research matters related to their project. Supervisors will also help students (a) decide on the scope of the project; (b) devise a project plan; (c) monitor their progress and adhere to target dates on provides; and (d) on how to tackle the writing up of the project report.

To support students in their studies and to allow access to module materials and course related information web-based teaching materials are used routinely. The modules' pages on the University's Virtual Learning Environment and/or the faculty's intranet pages are used as repositories for lecture notes, presentation transparencies, course/assessment schedules, coursework (including feedback) and occasionally for assessment purposes. The course recognises the importance of individuals being able to function equally well both as individuals and as members of team; thus, group activities are encouraged and promoted. To support and encourage student face to face interaction and collaborative work through exchange of emails, files, and online discussions, the facilities offered by the University's Virtual Learning Environment called Blackboard) are commonly utilised. Finally,

To summarise, teaching and learning strategies involve the use of

- case studies, to improve students' analytical and problem solving skills;
- use of specialised software tools and packages, such as FTK, EnCase and integrated systems such as Kali Linux;
- presentations from outside speakers with industrial experience, to enable students see how the taught material is applied in industry;
- team/group work, to enable students develop further their teamwork skills to work effectively in a professional environment;
- research methods involving the use of library and online sources to develop students research and analysis skills.
- presentations and academic report writing as part of the assignments set, to develop further these important skills.

Assessment

All of the taught modules in the programme are entirely assessed through coursework.

The approach taken in relation to assessment is that assessment is an integral part of the learning process; thus, assessment is designed to be fit-for-purpose in demonstrating the achievement of the specific module learning outcomes. The general principles governing assessment on the course are:

- a variety of assessment methods are employed fit-for-purpose to measure particular learning outcomes;

- the choice of assessment method(s) employed provides an opportunity for new learning and contributes to the learning process;
- timely and formative feedback is given for all assessments;
- assessment is criterion-based, i.e. assessed work is marked using clearly stated assessment criteria, finally,
- in selecting assessment methods consideration is given to maintaining an acceptable and balance assessment loading.

Course structure

In order to be awarded a Master's in Cyber Security and Forensics, a student must pass modules worth at least 180 credits and attempt modules worth no more than 240 credits. The modules a student needs to pass to be eligible for the award of the MSc qualification are all level 7 modules and include:

- all of the following core modules (120 credits):

Module Code	Module Title	UK Credits	ECTS	Pre/Co-requisites	Exam	Course work
7BUIS014W	Cyber Security Evidence and Procedure	20	10	NONE	–	100
7COSC003W	Fundamentals of Security Technology	20	10	NONE	–	100
7COSC007W	Internet Security	20	10	NONE	–	100
7BUIS019W	Research Methods and Professional Practice	0	0	NONE	–	100
7CSEF001W	Cyber Security and Forensics Project	60	30	Pass at least 100 credits incl. all the core modules	–	100

- and one of the following suggested groups of option modules (60 credits):

Digital Security Group (60 credits):

Module Code	Module Title	UK Credits	ECTS	Pre/Co-requisites	Exam	Course work
7BUIS022W	Cyber Security Applications	20	10	NONE	–	100
7CSEF002W	Cyber Security Threats and Counter-Measures	20	10	NONE	–	100
7BUIS020W	Risk Management	20	10	NONE	–	100

Digital Forensics Group (60 credits):

Module Code	Module Title	UK Credits	ECTS	Pre/Co-requisites	Exam	Course work
7COSC001W	Advanced Computer Forensics	20	10	NONE	–	100
7COSC006W	Computer System Tools	20	10	NONE	–	100
7COSC008W	Data Recovery and Analysis	20	10	NONE	–	100

Please note:

- Students may opt to take option modules from either of the above two groups provided they are timetabled in a way this is feasible.
- Not all option modules will necessarily be offered in any one year. The availability of modules depends on resources and on the numbers of students selecting a particular optional module.

Full time students are expected to complete the course within a calendar year, whereas students doing the course in part-time mode are normally expected to complete it over a two-year period. The above means that full time students cover the taught part of the course over the two semesters of an academic year and that they work on their project during the summer months of the same year. Part time students cover the taught part of the course over four semesters (two years) and that they are expected to work on their project during the summer months their second (last) year of their studies.

To pass a module, students must achieve an overall mark of 50% in the module. In addition, students must achieve at least 35% (qualifying mark) in each individual coursework component. Students, who fail to achieve the above, will be deemed as having failed the module and they may be offered a re-assessment.

At the discretion of the Assessment Board, a student may be re-assessed (re-sit) once only in any module other than the project module on each occasion that they attempt the module. The following guidelines can affect potential re-assessments (in what follows the term assessment component should be understood as coursework or grouping of assessment elements that the qualifying mark needs to be achieved):

- If an overall mark of 50% or above is achieved and there is a particular component where a score of less than 35% is achieved, then the student will be deemed as not having passed the module and they may be offered a re-assessment in that component.
- If an overall mark between 40% and 49% is achieved, then the student may be offered reassessment in the components where they have not achieved the passing mark.
- If an overall mark of less than 40% is achieved, then regardless of the score of individual components the student may have to retake the module with attendance.

The table below summarises the above guidelines:

		Assessment Component Mark	
		< 35%	**≥ 35%**
Overall Mark	50% or above	Reassess	Pass
	Between 40%-49%	Reassess	Reassess
	Less than 40%	Retake	Retake

Academic regulations

The MSc in Cyber Security and Forensics and its intermediate awards operate in accordance with the University's Academic Regulations and the Framework for Higher Education Qualifications in England, Wales and Northern Ireland published by the Quality Assurance Agency for Higher Education (QAA) in 2008.

All students should make sure that they access a copy of the current edition of the general University handbook called Essential Westminster, which is available at westminster.ac.uk/essential-westminster. The following regulations should be read in conjunction with the Modular Framework for Postgraduate Courses and relevant sections of the current Handbook of Academic Regulations, which is available at westminster.ac.uk/academic-regulations.

Award

To qualify for the award of MSc in Cyber Security and Forensics, a student must have:

- obtained a minimum of 180 credits at Level 7;
- attempt modules worth no more than 240 credits; and
  Note: A first attempt of any module will count as an attempt, and a re-attempt of any module that a student has failed will count as a further, separate attempt. Re-assessment following referral at the first sit will not count as a further separate attempt.
- satisfied the requirements contained within any course specific regulations for the relevant Course Scheme.

The University may award a Master’s Degree with

- Merit to a student whose marks average at least 60% across modules at Level 7, or
- Distinction to a student whose marks average at least 70% across the modules at Level 7.

Intermediate Awards

These are awards that students are not normally registered for in the first instance. A student’s registration may be changed to one of these exit awards, if a student has failed too many modules and cannot be considered for the target award s/he is registered for or a student claims such an award because s/he is withdrawing the course.

Postgraduate Diploma in Cyber Security and Forensics

In order to be awarded a Postgraduate Diploma (PgDip) in Cyber Security and Forensics, a student must pass modules worth at least 120 credits and attempt modules worth no more than 240 credits. The modules a student needs to pass to be eligible for the award of the Postgraduate Diploma (PgDip) in in Cyber Security and Forensics qualification are all level 7 modules and include:

- all of the following core modules (60 credits):

Module Code	Module Title	UK Credits	ECTS	Pre/Co-requisites
7BUIS014W	Cyber Security Evidence and Procedure	20	10	NONE

Module Code	Module Title	UK Credits	ECTS	Pre/Co-requisites
7COSC003W	Fundamentals of Security Technology	20	10	NONE
7COSC007W	Internet Security	20	10	NONE

– and three of the following optional modules (60 credits):

Module Code	Module Title	UK Credits	ECTS	Pre/Co-requisites
7COSC001W	Advanced Computer Forensics	20	10	NONE
7COSC006W	Computer System Tools	20	10	NONE
7BUIS022W	Cyber Security Applications	20	10	NONE
7CSEF002W	Cyber Security Threats and Counter-Measures	20	10	NONE
7COSC008W	Data Recovery and Analysis	20	10	NONE
7BUIS020W	Risk Management	20	10	NONE

The University may award a Postgraduate Diploma with

- Merit to a student whose marks average at least 60% across the modules contributing to the award, where the Diploma is the target award rather than an intermediate award conferred following failure in one or more modules, or
- Distinction to a student whose marks average at least 70% across the modules contributing to the award, where the Diploma is the target award rather than an intermediate award conferred following failure in one or more modules.

Postgraduate Certificate in Cyber Security and Forensics

In order to be awarded a Postgraduate Certificate (PgCert) in Cyber Security and Forensics, a student must pass modules worth at least 60 credits and attempt modules worth no more than 240 credits. The modules a student needs to pass to be eligible for the award of the Postgraduate Certificate (PgCert) in Cyber Security and Forensics qualification are all level 7 modules and include:

– both the following core modules (40 credits):

Module Code	Module Title	UK Credits	ECTS	Pre/Co-requisites
7COSC003W	Fundamentals of Security Technology	20	10	NONE
7COSC007W	Internet Security	20	10	NONE

– and one of the following optional modules (20 credits):

Module Code	Module Title	UK Credits	ECTS	Pre/Co-requisites
7COSC001W	Advanced Computer Forensics	20	10	NONE
7COSC006W	Computer System Tools	20	10	NONE
7BUIS022W	Cyber Security Applications	20	10	NONE
7BUIS014W	Cyber Security Evidence and Procedure	20	10	NONE
7CSEF002W	Cyber Security Threats and Counter-Measures	20	10	NONE
7COSC008W	Data Recovery and Analysis	20	10	NONE
7BUIS020W	Risk Management	20	10	NONE

The University may award a Postgraduate Certificate with

- Merit to a student whose marks average at least 60% across the modules contributing to the award, where the Certificate is the target award rather than an intermediate award conferred following failure in one or more modules, or
- Distinction to a student whose marks average at least 70% across the modules contributing to the award, where the Certificate is the target award rather than an intermediate award conferred following failure in one or more modules.

Support for students

Upon arrival, an induction programme will introduce students to the staff responsible for the course, the campus on which they will be studying, the Library and IT facilities and to the Faculty Registry. Students will be provided with the Course Handbook, which provides detailed information about the course. Students are allocated a personal tutor who can provide advice and guidance on academic matters.

Learning support includes four libraries, each holding a collection of resources related to the subjects taught at their Faculty. 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. They can also choose from several computer rooms at each campus where desktop computers are available with the general and specialist software that supports the courses taught at their Faculty. Students can also securely connect their own laptops and mobile devices to the University wireless network.

The University uses a Virtual Learning Environment called Blackboard where students access their course materials, and can communicate and collaborate with staff and other students.

Student Affairs provide advice and guidance on accommodation, financial and legal matters, personal counselling, health and disability issues, careers and the chaplaincy providing multi-faith guidance. The Student Affairs Hub is located at 101 New Cavendish Street, Cavendish House (1st Floor), with an additional office located at the Harrow Campus. More information can be found at: westminster.ac.uk/study/new-students/when-you-arrive

The University of Westminster Students' Union also provides a range of facilities to support all students during their time at the University. For further information please visit uwsu.com

Reference points for the course

Internally

- The University's Mission Statement
- The University's Quality Assurance and Enhancement Handbook
- The University's Handbook of Academic Regulations (2015)
- L & T Good Practice Guides produced by Westminster Exchange
- Learning & Teaching Guides for the Inclusive Curriculum for Disabled Students (2009) produced by ICDS Project Team
- Outcomes and actions of the Curriculum and Assessment Enhancement Workshop
- Academic staff research interests in Big Data, Data Science, Database Systems, Database Languages, Systems Architecture, Data Warehousing, Data Mining, Information Knowledge Management, etc.

Externally

- QAA Characteristics Statement UK Master's Degree, September 2015, available online www.qaa.ac.uk/en/Publications/Documents/Masters-Degree-Characteristics-15.pdf
- QAA UK Quality Code for Higher Education Part A: Setting and Maintaining Academic Standards, The Frameworks for Higher Education Qualifications of UK Degree-Awarding Bodies, October 2014, available online www.qaa.ac.uk/en/Publications/Documents/qualifications-frameworks.pdf
- QAA Guidance on Contact hours to Institutions, 2011, available online www.qaa.ac.uk/Publications/InformationAndGuidance/Documents/contact_hours.pdf
- QAA Guidance on contact hours to students , 2011, available online www.qaa.ac.uk/Publications/InformationAndGuidance/Pages/contact-hours-student.aspx
- QAA, Subject Benchmark Statement: Master's degrees in Computing, 2011, available online www.qaa.ac.uk/Publications/InformationAndGuidance/Documents/QAA386_Computing.pdf
- The Benchmarking Standards for Taught Masters Degrees in Computing, 2008 sponsored by CPHC and BCS,
- BCS, Guidelines on Course Accreditation – Information for Universities and Colleges, September 2015.
- SEEC Credit Level Descriptors 2001, Jan 2002.

Professional body accreditation

The course will be submitted for BCS accreditation during the next BCS accreditation visit in Autumn 2016. More information on BCS and membership paths can be found at www.bcs.org.

Quality management and enhancement

Course management

The Course Leader is responsible for the academic management and organisation of the course. The Course Leader, who is also the Admissions Tutor for the course, is assisted by an Examinations Officer and a Project Co-ordinator. The Course Team comprises the Course Leader and all the members of staff who teach on the course. Typically each module is delivered by a module team. Each module has a Module Leader, who is responsible for co-ordinating the module team and for the delivery, resourcing and smooth running of the module.

Course approval, monitoring and review

The course was initially approved by a University Validation Panel in 2008. The panel included internal peers from the University and external subject specialists from academia and industry to ensure the comparability of the course to those offered in other universities and the relevance to employers. Periodic course review helps to ensure that the curriculum is up-to-date and that the skills gained on the course continue to be relevant to employers.

The course is monitored each year by the Faculty to ensure it is running effectively and that issues which might affect the student experience have been appropriately addressed. Staff will consider evidence about the course, including the outcomes from each Course Committee, evidence of student progression and achievement and the reports from external examiners, to evaluate the effectiveness of the course. The Annual Monitoring Sub-Committee considers the Faculty action plans resulting from this process and the outcomes are reported to the Academic Council, which has overall responsibility for the maintenance of quality and standards in the University.

Student involvement in Quality Assurance and Enhancement

Student feedback is important to the University and student views are taken seriously. Student feedback is gathered in a variety of ways. The most formal mechanism for feedback on the course is the Course Committee. Student representatives will be elected to sit on the Committee to represent the views of their peer group in various discussions. The University and the Students' Union work together to provide a full induction to the role of the Course Committee.

All students are invited to complete a Module Feedback Questionnaire before the end of each module. The feedback from this will inform the module leader on the effectiveness of the module and highlight areas that could be enhanced. The University also has an annual Student Experience Survey which elicits feedback from students about their course and University experience.

Students meet with review panels when the periodic review of the course is conducted to provide oral feedback on their experience on the course. Student feedback from course committees is part of the Faculty's quality assurance evidence base.

For more information about this course:

Admissions Tutor: Paul Douglas
Dept of Computer Science
Faculty of Science and Technology
Tel: +44 (0) 20 7911 5000
Email: PDouglas@westminster.ac.uk

Course Enquiries:
Tel: +44 (0) 20 7915 5511
Email: admissions@westminster.ac.uk

Please note: This programme specification provides a concise summary of the main features of the course and the learning outcomes that a student might reasonably be expected to achieve and demonstrate if s/he takes full advantage of the learning opportunities that are provided. This specification should be read in conjunction with the Course Handbook provided to students and Module Handbooks, which provide more detailed information on the specific learning outcomes, content, teaching, learning and assessment methods for each module.