Course Specification

PART A: About the Course

1. **Qualification** (award and title and, where appropriate, Apprenticeship Standard title and code):

   BSc (Hons) Cyber Security

2. **Delivery Partners and Recognition:** *who delivers this course, where? Is it accredited by any professional bodies?*

Campuses/Partners	
University of West London RAK Branch Campus	

3. **Course Description:** *a short descriptive statement used for publicity* (max. 1150 characters):

Cyber security is essentially about the protection of information and information systems. On this course, students will learn how to perform this protective role, exploring different security technologies and studying management processes and control systems.

As studying for the course, students will:

- build the skills you need to design and develop modern secure systems;
- develop their appreciation of commercial and open-source cyber security equipment, software and services;
- learn management and applications central to cyber security issues
- develop interpersonal skills and business acumen.

The course will begin with an introduction to cyber security. Students will also learn about computing principles, including the essentials of programming and algorithms, software engineering, and mathematics and computer architecture.

Students will go on to build their knowledge in specialist modules that examine key topics in security. The computing modules will focus on skills in AI which has a close connection to security, while a group project will help them to develop team-working skills.

Finally, students will focus on advanced cyber security topics. This will help them to direct their studies so they reflect their interests and career ambitions. At the end of your course, students will design and develop a security-related project.

After completing the course, students will have the necessary knowledge and skills to embark on a career in cyber security.

4. Course Structure Diagram: *a visual overview of the programme of study*

Full-time September start. All modules are 20 credits except for L6 project which is 40 credits.

LEVEL 4

Semester 1	Semester 2
Core – Computer Architecture (CA) **CP4CS53E** (modified)	**Core –** Algorithms and Data Types (ADT) **CP4CS64E** (modified)
Core – Programming (PROG) **CP4CS61E** (modified)	**Core –** Information Systems and Databases (ISDB) **CP4CS54E** (modified)
Core – Mathematics for Computing (MATH) **CP4CS63E** (modified)	**Core –** Cyber Security in Society (CSS) **CP40070E** (modified)

LEVEL 5

Semester 1	Semester 2
Core – Theory of Computation (TC) **CP5NEW**	**Core –** Networks and Security (NS) **CP50088E**
Core – Applied Cryptography (AC) **CP50087E**	**Core –** Group Research Project (GPRJ) **CP5CS81E** (modified)
Core – Artificial Intelligence (AI) **CP5NEW**	**Core –** Cyber Threat Analysis (CTA) **CP50089E**

LEVEL 6

Semester 1	Semester 2
Core – Cyber Crime (CC) LW60074E (Law school)	**Core –** Enterprise Security Management (ESM) **CP60042E**

Core – Machine Learning (ML) **CP6NEW**	**Core –** Advanced Topics in Cyber Security (ATCS) **CP60041E**
Core - Project (PRJ, 40 credits – year long) **CP6CS46E**	

Full-time January starters will join the September cohort and start with semester 2.

5. Course Aims and Content by Level: *what is this course all about and how does it build and develop over time?*

The BSc (Hons) Cyber Security course aims to equip students with the knowledge and understanding of cyber security issues in relation to the design, development and use of information systems. The course will develop students' ability to recognise the legal, social, ethical and professional issues involved in the exploitation of cyber security technology and be guided by the adoption of appropriate professional, ethical and legal practices. The course is designed to meet industry needs/job market demands, and produce graduates who are informed and suitably equipped to meet the needs of the industry. The course will develop the critical skills and techniques that enable students to take up security related jobs/roles in a rapidly evolving and technologically diverse environment to appropriately solve typical cyber security problems. The course also develops the necessary competencies (including critical thinking skills and general skills) and provides a solid foundation for applied research in cyber security, with which student may go on to do further study in the MSc Cyber Security degree courses.

The BSc (Hons) Cyber Security course provides the professional education in the state-of-the-art theory and practice of cyber security, with well-balanced content on the concepts and principles, techniques and skills, as well as management and applications central to cyber security topics of both technical aspects and human dimensions. The content of the BSc (Hons) Cyber Security course by level is as follows:

LEVEL 4 In the first year of the course students will start to take an introductory security module, to gain fundamental understandings and skills on Cyber Security. The remaining modules of this year are shared with BSc (Hons) Computer Science course currently running at the School of Computing and Engineering, aiming to provide a solid grounding in Computer Science. It comprises modules covering the fundamentals of computing laying strong foundations for the rest of the course. This will include the essential aspects of programming and algorithms, software engineering, mathematics and computer architectures.	
LEVEL 5 In the second year of the course students will take a number of specialist modules on Cyber Security. Through these modules, students will gain good understandings and skills on the key topics of Cyber Security including cryptography, networking and system security, web and mobile security. Students will also have an opportunity to engage in group research project focusing on security relevant topics. As part of the module students will focus on research methodologies. The module will also prepare students for their final year project. The second year of the course also shares with BSc (Hons) Computer Science on some modules relating more specifically to AI and to developing skills in theoretical computer science, which are essential to explore the fundamental design of security systems.	
LEVEL 6 The third year of the course will focus on a range of specialised and advanced Cyber Security topics, and develop skills in research and critical reflection. Students will also be able to get some flavour of machine learning to ponder how AI and security interacts. In the final year project students will design and develop security-centric projects.	

6. Course Contact Hours: *how much time should I commit to this course?*

Learning hours are determined by credits. One credit is worth 10 learning hours, so a 20 credit module is 200 learning hours, a 30 credit module is 300 hours etc. This is the amount of time you should be prepared to commit to each module.

Learning hours are divided into: taught or 'contact' hours, i.e. the amount of time students spend in contact with academic staff, whether through face-to-face classes or online learning; and independent study, i.e. the amount of time students are expected to spend on their own study and assessment preparation. Some kinds of learning mix contact time and independent study, for instance presentations or workshops by invited experts, or sessions where you are working in groups on a project but can call on academic staff for advice or feedback on your work so far. You also have one-to-one time with academic staff in personal tutorials.

7. Course Learning Outcomes: *what can I expect to achieve on this course?*

	Level 4	Level 5	Level 6
Knowledge and understanding	A4.1 - Demonstrate key factual and conceptual knowledge in the field of computing. A4.2 - Apply concepts and techniques for developing and architecting software and hardware. A4.3 - Apply given techniques to analyse and test data with an appreciation of fundamental models and concepts. A4.4 - Build an appreciation of fundamental models and concepts underpinning computing and software programming and computer architectures.	A5.1 – Select and apply a range of procedures and techniques to model, design, and implement computer-oriented solutions to practical problems A5.2 – Distinguish and evaluate different theoretical frameworks to demonstrate knowledge and understanding in the computing industry A5.3 – Demonstrate and construct different paradigms for software development A5.4 – Implement the principles of object-oriented programming and design patterns and that underpin software development and ubiquitous computing	A6.1 – Exhibit in-depth knowledge of the computing industry and critically evaluate own skills and knowledge in this context for future career A6.2 – After critical analysis, select and apply a range of robust procedures and techniques to model, design, and implement computer-oriented solutions to practical problems A6.3 – Demonstrate the understanding of concepts and infrastructure underpinning security and artificial systems. A6.4 – Demonstrate the deployment of enterprise solutions and its security management issues.

	A4.5 - Apply the principles of algorithms and data structures that underpin software development A4.6 – Understand that information is an organizational asset that has utility, value and lifecycle, information has attributes relating to confidentiality, possession or control, integrity, authenticity, availability and utility, any of which can make it vulnerable to attack and thus need to be protected. A4.7 – Understand how to classify threats and example categories A4.8 – Understand the key factors to consider when creating a cybersecurity awareness or user education program	A5.5 – Demonstrate the understanding of group work and processes in a work environment. A5.6 – Understand different types of attacks which have different patterns and different steps, and attacks can be combined for greater effect A5.7 – Understand security controls can be categorised and selected on the basis of that categorisation	A6.5 – Specify, design and critically evaluate different programming paradigms for appropriate contextual deployment and software engineering. A6.6 – Understand the trade-offs for functionality, usability and security A6.7 – Understand the concept of residual risk and what it means to an organization A6.8 – Understand where technical controls cannot be used, other controls can be selected A6.9 – Understand the cybersecurity legal and ethical concerns, privacy as a special form of information protection. A6.10 – Understand the key elements of security governance and its role, the standards such as ISO/IEC cybersecurity governance, etc.

	A4.1 – CA, MATH, PRO, ADT, ISDB A4.2 – CA, PRO, ADT, ISDB A4.3 – ADT, ISDB, MATH, CSS A4.4 – CA, PRO, ADT, ISDB A4.5 – PRO, ADT, ISDB A4.6 – PRO, CSS A4.7 – CSS A4.8 – CSS	A5.1 – TC, AI, AC, NS, CTA, TP A5.2 – TC, AI, AC, NS, CTA, TP A5.3 – TC, AI, AC, NS CTA, TP A5.4 – TC, AI, AC, NS, CTA, TP A5.5 – GPRJ A5.6 – AC, NS, CTA A5.7 – AC, NS, CTA	A6.1 – ESM, CC, ATCS, PRJ, ML A6.2 – ESM, ATCS, PRJ, ML A6.3 – ESM, ATCS, PRJ A6.4 – ESM, ATCS, PRJ, ML A6.5 – ATCS, PRJ A6.6 – EMS, ATCS A6.7 – ESM, ATCS A6.8 – ESM, ATCS A6.9 – ESM, CC, ATCS A6.10 – ESM, CC, ATCS
Intellectual skills	B4.1 - Manipulate and use various tools and techniques for architecting given requirements B4.2 - Analyse a simple system in terms of given principles B4.3 - Investigate a problem, formulate solutions with justification of conclusions B4.4 - Specify a computing system in terms of basic	B5.1 – Evaluate alternative solutions and apply appropriate criteria in a variety of contexts B5.2 – Design, by the selection and application of appropriate techniques, a computer artefact B5.3 – Assess alternative approaches to the programming of software solutions	B6.1 – Employ the cognitive skills of critical thinking, analysis and synthesis including the capability to identify assumptions, evaluate statements in terms of evidence, to identify implicit values, to define terms adequately and to generalise appropriately. B6.2 – Manifest a critical awareness of current ethical, legal and quality frameworks

	hardware and software requirements B4.5 – Analyse the difference between threat, risk, attack and vulnerability	B5.4 – Ability to relate major engineering principles, management practice, and mathematical formalisms to software development B5.5 – Evaluate and select appropriate research methods in order to formulate a credible research proposal. B5.6 – Discuss the application of security techniques to demonstrate how controls can be selected, deployed and tested to minimise risk and impact B5.7 – Differentiate between controls to protect systems availability and reliability, controls to protect information, and controls to manage human behaviour B5.8 – Understand the role of security operation in monitoring, maintaining and evolving control. B5.9 – Understand how technical security controls	that apply to the development of systems by incorporation of these concepts across a range of business issues. B6.3 – Devise and apply concepts for machine learning and artificial intelligence. B6.4 – Critically analyse and apply concepts in software engineering and computer security to the practical design of elements of business solutions. B6.5 – Highlight the need for security architecture and its relevance to systems, service continuity and reliability B6.6 – Apply key steps in managing security incidents, the components and steps for a Business Continuity Plan/Disaster Recovery Plan B6.7 – Place security in an organisational context, respect for organisational needs, other individuals and confidential information

		work in detail/at an advanced level of understanding	
	B4.1 – CA, ISDB, CSS B4.2 - CA, MATH, PRO, ADT, ISDB, CSS B4.3 - CA, MATH, PRO, ADT, ISDB, CSS B4.4 - CA, PRO, ADT, ISDB B4.5 - CSS	B5.1 – TC, AI, AC, NS, CTA, GPRJ B5.2 – TC, AI, AC, NS, CTA, GPRJ B5.3 – TC, AI, AC, NS, CTA, GPRJ B5.4 – TC, AI, AC, NS, CTA, GPRJ B5.5 – GPRJ B5.6 – AC, NS, CTA B5.7 – AC, NS, CTA B5.8 – AC, NS, CTA B5.9 – AC, NS, CTA	B6.1 – ESM, CC, ATCS, PRJ, ML B6.2 – ESM, CC, ATCS, PRJ, ML B6.3 – PRJ, ML B6.4 – ESM, ATCS, PRJ B6.5 – ESM, ATCS B6.6 – ESM, ATCS B6.7 – EMS, CC, ATCS
Subject practical skills	C4.1 - Design, implement and test a simple computer-based solution and present results appropriately. C4.2 - Use appropriate techniques to analyse model, test data and to produce structured reports.	C5.1 – Develop a software artefact with an appropriate design for best practices as part of software services C5.2 – Analyse the technologies used to support requirements and construct software related to specified requirements C5.3 – Develop skills is the development of systems using	C6.1 – Plan, implement, monitor and complete a significant independent computing practical project under only limited guidance from academic supervisor C6.2 – Account for their professional conduct, particularly with respect to current ethical, legal and

	C4.3 – Apply knowledge on computer software and systems architectures C4.4 - Use basic tools to analyse and model secure systems. C4.5 - Identify different types of malware, their distribution mechanism and how they compromise information and systems.	mathematically modelling techniques C5.4 – Implement procedures and concepts for the development of software systems for secure distributed systems C5.5 – Critically evaluate and select recommended technologies needed to develop secure web and networking applications C5.6 – Apply technical security controls in practice and evaluate associated strengths and weaknesses	quality frameworks that apply within the computing industry C6.3 – Critically evaluate and recommend the technologies needed to develop secure artefacts C6.4 – Analyse requirements for, and evaluate and develop solutions to intelligent systems C6.5 – Analyse the key steps in a design process and where security considerations should be worked in. C6.6 – Design security controls can be implemented to protect systems and information C6.7 – Identify common trade-offs and compromises that are made in the security design and development process C6.8 - Demonstrate the knowledge of a security management framework and identify commonly used

			standards and areas of best practice C6.9 – Demonstrate the ability to describe the various tools that can be used in cybersecurity management C6.10 – Demonstrate an understanding of security compliance and its importance
	C4.1 - CA, MATH, PRO, ADT, ISDB C4.2 - CA, MATH, PRO, ADT, ISDB, CSS C4.3 - CA, MATH, PRO, ADT, ISDB, CSS C4.4 - MATH, CSS C4.5 - CSS	C5.1 – TC, AI, AC, NS, CTA, GPRJ C5.2 – TC, AI, AC, NS, CTA, GPRJ C5.3 – TC, AI, AC, NS, CTA, GPRJ C5.4 – TC, AI, AC, NS, CTA, GPRJ C5.5 – TC, AI, AC, NS, CTA, GPRJ C5.6 – AC, NS, CTA, GPRJ	C6.1 – ESM, CC, ATCS, PRJ, ML C6.2 – ESM, CC, ATCS, PRJ, ML C6.3 – ESM, CC, ATCS, PRJ C6.4 – ESM, ATCS, PRJ, ML C6.5 - ESM, CC, ATCS, PRJ C6.6 - ESM, CC, ATCS, PRJ C6.7 - ESM, CC, ATCS, PRJ C6.8 – ESM, CC, ATCS, PRJ C6.9 – ESM, CC, ATCS, PRJ C6.10 - ESM, CC, ATCS, PRJ

Transferable skills	D4.1 - Adopt a flexible, adaptable and professional attitude towards learning and the development of skills D4.1 - Manage time and resources to meet deadlines D4.3 - Present information in effectively in a clear and concise manner using a variety of formats. D4.4 - Recognise their own, and others, strengths and weaknesses	D5.1 – Interact effectively in a variety of different learning groups in both real and virtual contexts D5.2 – Efficiently apply appropriate technology to facilitate and manage own learning D5.3 – Communicate in a clear and concise manner using appropriate technical D5.4 – Work effectively with others D5.5 – Critically evaluate the practical experiences and knowledge gained and how the work experience has enhanced their own personal development.	D6.1 – Exercise initiative and personal responsibility for the management of own learning D6.2 – Demonstrate the ability to manage independent learning necessary for continued professional development D6.3 – Reflect on personal attainment and appropriately apply learning experiences to inform and enhance subsequent professional practice
	D4.1 - CA, MATH, PRO, ADT, ISDB, CSS D4.2 - CA, MATH, PRO, ADT, ISDB, CSS D4.3 - CA, MATH, PRO, ADT, ISDB, CSS	D5.1 – TC, AI, AC, NS, CTA GPRJ D5.2 – TC, AI, AC, NS, CTA GPRJ D5.3 – TC, AI, AC, NS, CTA, GPRJ	D6.1 – ESM, CC, ATCS, PRJ, ML D6.2 – ESM, CC, ATCS, PRJ, ML D6.3 – ESM, CC, ATCS, PRJ, ML

	D4.4 - CA, MATH, PRO, ADT, ISDB, CSS	D5.4 – TC, AI, AC, NS, CTA, GPRJ	

8. Learning, Teaching and Assessment Strategies: *how will I learn, how will my learning be assessed, and why are these the most appropriate methods?*

Teaching and Learning Approaches

The underlying philosophical approach to teaching and learning on this course is consistent with that of the university. Design of the modules making up the course is assessment driven, in that they are designed from learning outcomes and assessment upwards. Students on the course will be encouraged to take responsibility for their own learning whilst still being supported by subject tutors. Students are encouraged to immerse themselves in the subject area.

There is an appropriate balance of theory and practice, and in order to be successful students will need to demonstrate appropriate levels of analytical, critical and reflective skills alongside a professional level of practical skills and knowledge. Teaching and learning on the course is underpinned by the research and development activities of the course team.

Teaching methods include lectures, whole group information-giving sessions, workshops, tutorials, practical work, and blended e-learning and group critiques.

Practical work

The practical work will reflect real-world techniques that practitioners would encounter in industry.

Blended E-Learning

The University of West London is now relatively experienced in the use of an e-Learning platform – Blackboard to support traditional HE delivery methods. Within UWL, The School of Computing and Engineering is perhaps one of the most mature users of Blackboard. This is evidenced by:

- Contributions that staff members have made to the university wide staff development programmes for e-learning notably in the area of assessment using On-line Discussion Forums.
- Use of Blackboard on most UG and PG modules at varying levels of sophistication.
- Provision of specialist advice in eLearning to the University with respect to integration of Portal technology with Blackboard.

As noted above, the use of Blackboard and eLearning elements varies with each module. But it is useful to note that within the five level model proposed by van der Craats, McGovern and Pannan (2002) , most staff are at least at level 2 (Document

Distribution of learning materials) and several are at the level 3 - Enhanced Face To Face Level (use of discussion boards, formative assessment, community support). There are also plans to consider full e-Learning based delivery of several of the modules of the Masters Programmes.

This level of maturity and experience within the subject group will enable the use of Blackboard to support the learning requirements all students on postgraduate degrees. In particular, the blended e-learning approach will be of significant value to work based students.

From a strategy perspective, our goal is to progress staff development in eLearning such that most if not all staff are at level 3 – indicative of a truly blended approach.

As the knowledge and experience to enable this to happen resides within the subject group this will happen naturally over time, but we will endeavour to put in place, mechanisms such as module team structures, specific staff development workshops and encourage attendance at faculty and university level staff development opportunities. The use of professional tools and technologies seek to provide the knowledge and skills required in computing industry. These tools are thought on most modules.

Assessment Approaches

Coursework based assessment is designed, where possible to simulate the variety of tasks that graduates from the course may encounter in relevant employment. Where necessary other academic assessment devices, such as a formal examination are also used.

During the level 4, much of the assessment is by means of portfolio development which may take the form of class tests, presentations, or practical activities. As the year develops and the confidence of the student increases, the assessment will have a more conventional output e.g. formal reports and other documentation.

In subsequent years, assessment types include the following:

- Analysis and design and the production of appropriate artefacts
- Portfolio of work
- Presentations to tutors and peers
- Development of design specifications
- Critiques of own and peer work
- Major implementation project
- Examinations and class tests

Wherever possible the students will be encouraged to relate theory to practice and to reflect on practice experienced. This challenge will be addressed by developing a student-centred approach to learning and teaching. This has involved the introduction of a range of specific techniques including problem-based learning and case studies, which will inform the development of the assessment strategy. Its intension is to make the curriculum interesting and relevant to diverse groups of students. Social constructivism emphasises the importance of student learning through interaction with teachers and other students.

The assessment material for each module will be distributed to the students at the commencement of the module. This material will include a complete set of requirements and dates for completion as well as a marking scheme and associated performance criteria.

During the delivery of each module students will receive feedback on their performance on class exercises. These exercises will not normally be graded for assessment purposes. However, the work completed during these exercises may form part of the work to be handed in for the module assessment at the completion of the module.

There are a variety of mechanisms by which feedback on assessments is provided to students. Where assessments are portfolio based, formative assessment on elements of draft submissions is provided during class or via email. Additionally, portfolio based assessments allow work to be submitted in stages where each element submitted receives summative feedback.

Student feedback will also be provided via the Blackboard E-Learning Platform. This is particularly useful where there are trends in student work and formative feedback can be provided to class groups. Formative feedback is available during dedicated class sessions and via email and pre-arranged meetings with course tutors.

Written feedback is provided on assessed work via Rubrics on Blackboard. Additional feedback is also provided in a general form as part of the module leader's report or during course committee meetings.

Level 4

Level 4 modules cover the basic theoretical concepts, programming, and Mathematics, and introduction to security. Appropriate software tools are introduced and incorporated as part of the teaching materials to provide the skills needed to design artefacts, and solve Computing specific tasks, and for students to be able to evaluate relevant information and ideas.

Assessments are designed to simulate a variety of tasks including problem solving activities, and to apply concepts and techniques for developing and architecting software and hardware.

All of the assessment is by means of written assignment reports and portfolio development, and in-class assessment which may take the form of class tests, presentations, or practical activities. Assignments are designed with elements of programming exercises and problem solving. They provide an ability, for students, to present and evaluate results and solutions and to make judgements in accordance with the theories and concepts presented in the modules.

Level 5

Wherever possible the students will be encouraged to relate theory to practice and to reflect on practice experienced. This challenge will be addressed by developing a student-centred approach to learning and teaching. This has involved the introduction of a range of specific techniques including problem-based learning and case studies, which will inform the development of the assessment strategy. Its intention is to make the curriculum interesting and relevant to diverse groups of students.

Students gain understanding of theoretical concepts that are covered in understanding a list of well-established security services and mechanism, while combining experimental analysis and practices to apply the theory into practice.

As part of the Group Research Project module students design and develop an artefact, using case studies and requirements elicitation techniques and communicating and collaborating by means of appropriate software tools. They will also begin investigating a topic and produce a draft project proposal for their final year project.

Level 6

During the final year of the course, students engage on their final year-long project. Project titles and topics are discussed with supervisors, and aims and objectives are set. As part of the project work, the theory and concepts applied by designing and developing an artefact, with opportunity to exercise initiative and personal responsibility for the management of own learning.
As part of the project work, students will critically evaluate and recommend the technologies used and incorporated for the artefact.

The security management framework and tactics in an organisation are delivered by means of case studies, which aims to allow students to have their own ideas of evaluating security risk in the context of real world organizations.

The research effort within the school contributes towards the curriculum, and at level 6, students engaged in providing solutions to given tasks, and to deploy accurately the established techniques of design and analysis. This is reflected in the module of advanced topics in cyber security.

9. Formal and Informal Links with External Organisations/Industrial Partners: *what opportunities are there for me to interact with professional contacts?*

The links and ongoing dialogues established by the team with the computing industry and other educational establishments form an essential and valued element in the design of the course material and the delivery of the course. Constant development and refinement of the modules will be a feature of the course in order to update and maintain its currency and a wholly contemporary relationship with the design industries the students aspire to enter on graduation. In addition to those links forged by staff with key industrial practitioners, students are expected as a matter of course to begin to make contact with relevant industrial links as part of the push to develop their presentation skills. A key element in this is the continuing professional practice by the delivery team which covers practical updating, individual research, theoretical enquiry in relevant areas as well as, most importantly, being creative and exhibiting practitioners in their chosen industry based and/or technical fields. This course will benefit from the work research centres and groups within the School. The School currently has a number of Research Centres, including Cyber Security Research Centre.

The school has a strong link with its industry partners through the Computing Industrial Consultative Committee panel with regular annual meetings arranged per each academic year where the content of courses and subjects are discussed. The aim is to ensure the course delivers skills required in the industry. Furthermore, guest lectures are delivered by our industry partners to present topics of current subject interest in the market.

10. Admissions Criteria: *what qualifications and experience do I need to get onto the course?*

112 UCAS tariff points at Level 4 GCSE English and Maths with grade C. The professional/work/life experiences of the mature students and their ability to engage with, and benefit from, the course wishing to apply will be taken into account. They will only be offered a place if they are able to demonstrate a level of intellectual curiosity and organisational ability such that they have the potential to be successful on the course.

11. Student Support Arrangements, including 'in-company' support for Apprenticeships and PDP: *what kinds of academic and pastoral support and advice are available?*

STUDENT SUPPORT

University-wide Support Services for all students:

- Careers and Employment Services
- Student Advice
- Accommodation Service
- Counselling
- Students' Union
- Mentoring

Student advice, help and support is further detailed in the Student Handbook with regard to University facilities, services and current policies.

The Engagement Service is available to all UWL students working at any level and on any course. The Service offers easily accessible support so that students can reach their full potential.

Academic Support Opportunities include:

- Daily Academic Drop-in Support
- Academic Skills workshops
- Peer Mentor Pairing
- Maths Support

Daily Academic Drop-in Support

The Drop-in Support Sessions offer daily opportunities for students to seek guidance and academic support with no appointment required. The Drop-in Support sessions provide students with an easily available space and opportunity to seek solutions and gain personal academic advice whenever needed. Students attend to both overcome challenges and to build on their success. Many report that attending a drop-in has helped to dramatically reduce their anxiety and raise their confidence.

Academic Skills Workshops

The Academic Skills workshops are delivered throughout the year, helping students to develop skills relevant to their degree. Some aspects of a student's course may be challenging, or the student may have been out of education for some time. The workshops have been developed so that they include a theoretical element followed by an hour of supported practical study, where the theory can be applied and questions asked. Examples of workshops include: Time Management and Organising Your Studies, Report Writing, How to Write Critically, Group Work and Presentation Skills.

Peer Mentoring
Peer mentoring offers students the opportunity to be paired with another student, studying within the same academic school, who can support them by sharing their own experiences of the course and UWL. Students can request a mentor and it has been shown to be one of the best ways to help students acclimatise to university life and maximise their student experience, academically and socially. Students are paired with a peer mentor who can share their experience and provide another perspective on the School, the subject area and the course through regular meetings.
As student's progress through their course they can also volunteer to be peer mentors and support other students. Peer mentoring is highly valued by many employers and is a highly rewarding experience for all involved.

Maths Support
UWL students face varied maths challenges on their courses so UWL has enhanced the support available. A Maths specialist offers sessions to students from across the University. Support sessions are available 1:1 or in groups and allow students to ask further questions relating to the taught material during lectures, to bridge their gaps in knowledge and cement their understanding of mathematical concepts, numeracy and statistics.

Undergraduate and taught postgraduate courses
The University-wide support framework encompasses:

- Induction
- Course Leaders
- Module Leaders
- Personal Tutors
- VLE (Blackboard)
- In-course learning skills development*
- Personal Development Planning (PDP)**

*Learning skills include critical appraisal, reflection, literature searching, information technology, peer review, group work, presentation, research, practice/professional skills, note-taking, writing skills, electronic information retrieval, communication skills and independent study at home.
**PDP has been formalised on undergraduate degree courses via the Personal Tutorial system delivered through levels 4-6. These tutorials are designed to support the development of academic skills (at level 4) employability (at level 5) and personal reflection and research enquiry linked to career options (at level 6). PDP is developed informally in other areas of learning through students' development of personal skills such as time management, leadership, and teamwork. Guest speakers and field visits provide students with networking opportunities.

12. Assessment Matrix: *a list of all the assessments on the course, along with how much they count for and where they come in the year.*

Module Title and Code	Core /Optional (write C or O)	Credit	Assessment Type (choose from the dropdown list)	Weighting (%)	Overall pass mark	Minimum percentage (PSRBs and Apprenticeships only)	Apprenticeships Only: contributes to 'End-Point Assessment' (write YES or NO)	Submission: Week Number (indicative)
Level 4								
CP40053E **Computer Architecture**	C	20	*Portfolio*	**100**	40			**Week 16**
CP40061E **Programming**	C	20	*Portfolio*	**100**	40			**Week 16**
CP40063E **Mathematics for Computing**	C	20	*Portfolio*	**100**	**40**			**Week 16**
CP40054E **Information Systems and Databases**	C	20	*Portfolio*	**100**	**40**			**Week 16**
CP40064E **Algorithms and Data Types**	C	20	*Portfolio*	**100**	**40**			**Week 16**

Module Title and Code	Core /Optional (write C or O)	Credit	Assessment Type (choose from the dropdown list)	Weighting (%)	Overall pass mark	Minimum percentage (PSRBs and Apprenticeships only)	Apprenticeships Only: contributes to 'End-Point Assessment' (write YES or NO)	Submission: Week Number (indicative)
CP40070E **Cyber Security in Society**	C	20	*Portfolio*	**100**	**40**			**Week 16**
Level 5								
CP5NEW **Theory of Computation**	**C**	**20**	*Portfolio*	**50**	**40**			**Week 12**
			Written examination	**50**	**40**			**Exam Week**
CP50088E **Networks and Security**	**C**	**20**	*Portfolio*	**50**	**40**			**Week 10**
			Portfolio	**50**	**40**			**Week 16**
CP5NEW **Artificial Intelligence**	**C**	**20**	*Written assignment*	**50**	**40**			**Week 11**
			Written examination	**50**	**40**			**Exam Week**
CP50087E **Applied Cryptography**	**C**	**20**	*Portfolio*	**40**	**40**			**Week 10**
			Written examination	**60**	**40**			**Week 16**
CP50081E	**C**	**20**	*Written assignment*	**100**	**40**			**Week 14**

Module Title and Code	Core /Optional (write C or O)	Credit	Assessment Type (choose from the dropdown list)	Weighting (%)	Overall pass mark	Minimum percentage (PSRBs and Apprenticeships only)	Apprenticeships Only: contributes to 'End-Point Assessment' (write YES or NO)	Submission: Week Number (indicative)
Group Research Project								
CP50089E **Cyber Threats Analysis**	**C**	**20**	*Written assignment*	**50**	**40**			**Week 10**
			Written assignment	**50**	**40**			**Week 16**
Level 6								
CP60046E **Project**	**C**	**40**	*Written assignment*	**20**	**40**			**Semester 1, Week 14**
			Written assignment	**60**	**40**			**Semester 2, Week 14**
			Oral assignment	**20**	**40**			**Semester 2,** **Week 16**
CP6NEW **Machine Learning**	**C**	**20**	*Written assignment*	**100**	**40**			**Week 13**

Module Title and Code	Core /Optional (write C or O)	Credit	Assessment Type (choose from the dropdown list)	Weighting (%)	Overall pass mark	Minimum percentage (PSRBs and Apprenticeships only)	Apprenticeships Only: contributes to 'End-Point Assessment' (write YES or NO)	Submission: Week Number (indicative)
LW60074E **Cyber Crime**	**C**	**20**	*Written assignment*	**50**	**40**			**Week 10**
			Portfolio	**50**	**40**			**Week 16**
CP60042E **Enterprise Security Management**	**O**	**20**	*Portfolio*	**100**	**40**			**Week 16**
CP60041E **Advanced Topics in Cyber Security**	**O**	**20**	*Portfolio*	**100**	**40**			**Week 16**

13. External Examiner Arrangements: *who checks the standards and quality of the course?*

External examiners are attached to all modules at level 5 and level 6 as per the university regulations. They are responsible for assessing the quality of the programme and the consistency of standards across all levels.

External examiners are selected on the basis of their subject expertise and are subject to scrutiny by a division of the University's Academic and Quality Control Department – External Examiner's Advisory Committee (EEAC). External examiners are proposed by the College and if accepted by EEAC are in position for four years.

PART B: Key Information

1.	**Awarding Institution**	University of West London
2.	**UWL School/College**	SCE
4.	**Academic Partners and type of arrangement**	University of West London RAK Branch Campus, UAE
5.	**Course recognised by**	Click here to enter text.
6.	**Sites of delivery**	Click here to enter text.
7.	**Modes and duration of delivery**	Full time = 3 years - *BSc (Hons) Cyber Security* Click here to enter text.
8.	**Sequencing**	*September only start*
	Sequencing	*September and January start* *BSc (Hons) Cyber Security*

9.	**Final enrollable award(s)**	*BSc (Hons) Cyber Security*
10.	**Level of final award**	6
11.	**Credit for final award (CATS and ECTS)**	BSc (Hons) Cyber Security = 360 CATS/180 ECTS
12.	**Exit awards and credits**	BSc Cyber Security = 360 credits at level 4, 5 and 60 at level 6 Dip HE Cyber Security = 240 credits at levels 4 and 5. Cert HE Cyber Security = 120 credits at level 4
13.	**UCAS code(s) (UG programmes)**	
14.	**QAA Subject Benchmarking Statement**	Click here to enter text. Computing (2016) https://www.qaa.ac.uk/docs/qaa/subject-benchmark-statements/sbs-computing-16.pdf?sfvrsn=26e1f781_12 https://www.qaa.ac.uk/docs/qaa/subject-benchmark-statements/subject-benchmark-statements.pdf?sfvrsn=1656ff81_2

15.	**Apprenticeship Standard title and code**	N/A		
16.	**Course-specific Regulations**	Standard UWL regulations apply		
17.	**Language of study**	English		
18.	**Original approval Date**	Click here to enter text.	**Last Revision Date**	Click here to enter text.

PART C: Record of Approved Modifications

Approved Modifications to Course Specification since Validation/last review					
Course Specification Title	**Module Level and title**	**Brief Outline of Modification**	**Approval by School/College Quality Committee**	**Approval effective from**	**Student cohort affected**
Specify award titles/routes affected by change BSc (Hons) Cyber Security	Level 4: All Assessments changed to 100% Portfolio Level 5 • Team Project renamed to **Group Research Project**; incorporated research methodology elements into the module. • Mobile Application Development replaced with **Theory of Computation**	Following our recent Course Re-approval event (23rd May 2019), a few changes to the Cyber Security course have been inevitable in order to keep the delivery of modules consistent. This is particularly for modules that are to be shared across many courses	*Date and meeting minute* SCE School Executive June 2019	September 2019	*e.g. students entering Level 5 from AY2018* • All students entering Level 4,5,6 from Sept 2019Team Project renamed to **Group Research Project**; incorporated research methodology elements into the module. • Mobile Application Development replaced with

	• Distributed Computing replaced with **Artificial Intelligence** • Web and Mobile App Security replaced with **Cyber Threat Analysis** Level 6: • Natural Language Interface moved to semester 1 and replaced by **Machine Learning** • Enterprise Security module is moved to semester 2 delivery • The assessments for the module of Advanced Topics in Cyber Security is changed to portfolio with 100% weight				**Theory of Computation** • Distributed Computing replaced with **Artificial Intelligence** Web and Mobile App Security replaced with **Cyber Threat Analysis**