Bournemouth University

KEY PROGRAMME INFORMATION

Originating institution(s) Bournemouth University	**Faculty responsible for the programme** Faculty of Science and Technology
Final award(s), title(s) and credits BSc (Hons) Networks and Cyber Security – 120 (60 ECTS) Level 4 / 120 (60 ECTS) Level 5 / 120 (60 ECTS) Level 6 credits	
Intermediate award(s), title(s) and credits Dip HE Cyber Security – 120 (60 ECTS) Level 4 / 120 (60 ECTS) Level 5 credits Cert HE Computing – 120 (60 ECTS) Level 4 credits	
UCAS Programme Code(s) (where applicable and if known) G610	**HECoS (Higher Education Classification of Subjects) Code and balanced or major/minor load.** 100365 100376
External reference points • The UK Quality Code for Higher Education; • Chapter A1: The National Level (incorporating the Framework for Higher Qualifications (FHEQ) in England, Wales and Northern Ireland); • Chapter A2: The Subject and Qualification Level (incorporating the Subject benchmark statements for Computing (2022)); • BCS – The Chartered Institute for IT guidelines • United Nations Sustainable Development Goals (SDGs) • The Cyber Security Body Of Knowledge www.cybok.org	
Professional, Statutory and Regulatory Body (PSRB) links Click here to enter text.	
Places of delivery Bournemouth University, Talbot Campus	
Mode(s) of delivery Full-time/Full-time sandwich	**Language of delivery** English
Typical duration ***Select a typical duration as applicable*** UG September start (3 years full time or 4 years full time with 30 weeks sandwich placement)	
Date of first intake September 2023	**Expected start dates** September 2023
Maximum student numbers N/A	**Placements** 30 weeks, optional
Partner(s) N/A	**Partnership model** N/A
Date of this Programme Specification March 2025	
Version number 1.1-0925	

Approval, review or modification reference numbers E212216 EC 2223 09 EC 2223 16 EC 2223 32 EC2223 48, approved 02/10/2023 FST2425 21, approved 26/03/2025, previously 1.0
Author Wei Chai

© Bournemouth University 2022

PROGRAMME STRUCTURE

Programme Award and Title: BSc (Hons) Networks and Cyber Security								
Year 1/Level 4								
Unit Name	**Core/ Option**	**No. of Credits**	**Assessment Element Weightings**			**Expected Contact hours per unit**	**Unit Version No.**	**HECoS Code** (plus balanced or major/ minor load)
			Exam 1	**Cwk 1**	**Cwk 2**			
Computer Fundamentals	Core	20	50%	50%		36	3.0	100734 100735
Mathematics for Computing	Core	20	50%	50%		36	1.0	100400
Programming	Core	20	50%	50%		36	1.0	100956
Introduction to Cyber Security	Core	20		100%		36	1.0	100376
Network Essentials	Core	20		100%		36	1.0	100365
Computing and Society	Core	20		100%		36	1.0	100631 100367
Progression requirements: Requires 120 credits at Level 4 **Exit qualification:** Cert HE Computing (requires 120 credits at Level 4)								

© Bournemouth University 2022

Year 2/Level 5								
Unit Name	**Core/ Option**	**No. of Credits**	**Assessment Element Weightings**			**Expected Contact hours per unit**	**Unit Version No.**	**HECoS Code** (plus balanced or major/ minor load)
			Exam 1	**Cwk 1**	**Cwk 2**			
Communications and Networking	Core	20		100%		36	1.0	100365
Security Operations (SecOps)	Core	20		100%		36	1.0	100376
Software Engineering	Core	20	30%	70%		36	2.0	100374
Network and Cyber Management	Core	20		100%		36	1.0	100365 100376
Technological Innovations in Cyber Security	Core	20	30%	70%		36	1.0	100360 100373
Software Business	Core	20		100%		36	1.0	100360
Progression requirements: Requires 120 credits at Level 4 and 120 credits at Level 5 **Exit qualification:** Dip HE Cyber Security (requires 120 credits at Level 4 and 120 credits at Level 5)								
Compulsory/Optional placement year in industry/business: Students who successfully complete the one year placement will be awarded a degree in sandwich mode. **Progression requirements:** Satisfactory completion of a minimum 30-week placement (up to a year) in industry/business and placement report.								

© Bournemouth University 2022

Year 3/4/Level 6								
Unit Name	**Core/ Option**	**No. of Credits**	**Assessment Element Weightings**			**Expected Contact hours per unit**	**Unit Version No.**	**HECoS Code** (plus balanced or major/ minor load)
			Exam 1	**Cwk 1**	**Cwk 2**			
Human Computer Interaction	Core	20		100%		36	1.0	100736
Internet and Wide Area Networks	Core	20		100%		36	1.0	100365
Data Visualisation & Storytelling	Option	20		100%		36	1.0	100632 100755
Digital Innovation and Transformation	Option	20		100%		36	1.0	100362 101221
Deep Learning and Applications	Option	20		100%		36	1.0	100359 100992
Systems Development	Option	20		100%		36	1.0	100374 100956
Digital Futures	Core	20		100%		36	1.0	100373 100440
Individual Project	Core	40		100%		21	1.0	100358 (major) 100812 (minor)
Exit qualification: BSc (Hons) Networks and Cyber Security **Sandwich UG award:** Requires 120 credits at Level 4, 120 credits at Level 5, 120 credits at Level 6 and successful completion of a placement year. **Full-time UG award:** Requires 120 credits at Level 4, 120 credits at Level 5 and 120 credits at Level 6 .								

© Bournemouth University 2022

AIMS OF THE DOCUMENT

The aims of this document are to:

- define the structure of the programme;
- specify the programme award titles;
- identify programme and level learning outcomes;
- articulate the regulations governing the awards defined within the document.

AIMS OF THE PROGRAMME

The BSc (Hons) Networks and Cyber Security programme is designed to equip students with in-depth knowledge and technical skills relevant to computer networks and cyber security. This is in response to the increasing needs for workforce with expertise in this area as networks have become ubiquitous and tightly integrated to our lives and daily operations of all industries.

The programme will cover a broad range of topics ranging from theoretical aspects including the networking and security principles and concepts to practical aspects including network design and security operations. Throughout the programme, emphasis is placed on detailed secure network design, implementation, management and performance evaluation while also equip graduates with wider knowledge and appreciation on the societal and economic values of secure networks.

Graduates will learn relevant principles and practices as well as the latest networking and cyber security paradigms that will allow them to understand and design current and future network systems taking into account modern business or organizational settings including the legal and ethical aspects of computer network operation and management, such as security, resilience and issues of disaster recovery.

ALIGNMENT WITH THE UNIVERSITY'S STRATEGIC PLAN

The BSc (Hons) Networks and Cyber Security programme is informed by and well aligned with Bournemouth University's 2024 strategic plan and the fusion of excellent teaching, world-class research and professional practice that is at the heart of the institution's visions and values. It promotes the digital & technological futures as well as the global security themes along with internal partnerships between faculties at Bournemouth University. Students are supported by academics with a wealth of industry experience, many of whom are actively engaged in various network- and security-related projects with several external organisations. Academics delivering the programme are actively engaged in cutting edge research, while students are encouraged to participate in a range of co-creation and co-publication projects. The programme's innovative pedagogic approach offers students the opportunity to learn by engaging in a series of practical, industry focused tasks. These are aimed at equipping students with the full range of skills necessary to succeed in the contemporary ICT environment, and are informed by the academic team's own industrial experience as well as by a network of industry contacts, who may also contribute directly to the programme by delivering guest lectures.

LEARNING HOURS AND ASSESSMENT

Bournemouth University taught programmes are composed of units of study, which are assigned a credit value indicating the amount of learning undertaken. The minimum credit value of a unit is normally 20 credits, above which credit values normally increase at 20-point intervals. 20 credits is the equivalent of 200 study hours required of the student, including lectures, seminars, assessment and independent study. 20 University credits are equivalent to 10 European Credit Transfer System (ECTS) credits.

The assessment workload for a unit should consider the total time devoted to study, including the assessment workload (i.e. formative and summative assessment) and the taught elements and independent study workload (i.e. lectures, seminars, preparatory work, practical activities, reading, critical reflection, *practice (if relevant)*).

© Bournemouth University 2022

Assessment per 20 credit unit should normally consist of 3,000 words or equivalent. Dissertations and Level 6 and 7 Final Projects are distinct from other assessment types. The word count for these assignments is 5,000 words per 20 credits, recognising that undertaking an in-depth piece of original research as the capstone to a degree is pedagogically sound.

STAFF DELIVERING THE PROGRAMME

Students will usually be taught by a combination of senior academic staff with others who have relevant expertise including – where appropriate according to the content of the unit – academic staff, qualified professional practitioners, demonstrators/technicians and research students.

© Bournemouth University 2022

INTENDED LEARNING OUTCOMES – AND HOW THE PROGRAMME ENABLES STUDENTS TO ACHIEVE AND DEMONSTRATE THE INTENDED LEARNING OUTCOMES

PROGRAMME AND LEVEL 6 INTENDED PROGRAMME OUTCOMES

A: Subject knowledge and understanding This programme/level provides opportunities for students to develop and demonstrate knowledge and understanding of*:*	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:
A1 Principles and techniques of networks and cyber security-based research **A2** Enabling technologies for network and cyber security applications **A3** A rigorous engineering approach to investigating and solving networks and cyber security problems such as those in the Internet, enterprise networks, cyber physical systems contexts; **A4** The management and development of IT solutions to address networks and cyber security or other problems; **A5** The professional, legal & ethical responsibilities of network and cyber security personnel within the organisational, technical and global contexts in which networks and cyber security are applied.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (A1 – A5); • seminars (A1 – A5); • directed reading (A1-A5); • Use of VLE (A1 – A5) • independent research (for dissertation) (A1 – A5).
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (A1 – A5); • coursework (A1 – A5); • dissertation (A1 – A5).
B: Intellectual skills This programme/level provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level outcomes:
B1 Critically thinking, problem-solving and decision-making to solve complex networks and cyber security problems; **B2** Analyse, interpret, synthesise and critically evaluate information from current research; **B3** Critically evaluate and justify alternative approaches to solutions development; **B4** Formulate, plan, execute, and report on a networks and cyber security project involving original contributions; **B5** Communicate findings to professional and academic standards.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (B1 – B5); • seminars (B1 – B5); • directed reading (B1 – B5); • use of the VLE (B2 – B5);

© Bournemouth University 2022

	• independent research (for dissertation) (B1 - B5).
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (B1- B5); • coursework (B1 – B5); • dissertation (B1 – B5).
C: Practical skills This programme/level provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:
C1 Retrieve, select and evaluate information from a variety of sources ; **C2** Analyse, specify, design and implement networks and cyber security applications to meet business goals; **C3** Select appropriate methods and tools for solving networks and cyber security problems; **C4** Plan, monitor and evaluate the progress of a network and cyber security solution	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (C1 – C4); • seminars (C1 – C4); • independent research for empirical dissertation (C1 – C4);
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (C1 – C4); • coursework (C1 – C4); • dissertation (C1 – C4).
D: Transferable skills This programme/level provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:
D1 Demonstrate problem solving skills and the application of knowledge across the discipline areas. **D2** Gather, select, and analyse a range of experimental and fieldwork data and present professionally using appropriate media. **D3** Structure and communicate ideas professionally and effectively to appropriate professional and academic standards.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (D1 - D5); • seminars (D1- D5); • use of the VLE (D1 - D5); • directed reading (D1- D5).

© Bournemouth University 2022

D4 Demonstrate initiative, self direction and exercise personal responsibility for management of own learning. **D5** Distil, synthesise and critically analyse alternative approaches and methodologies to problems and research results reported in literature and elsewhere.	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework essays (D1 - D5); • examinations (D1, D3); • dissertation (D1- D5).

LEVEL 5/DipHE INTENDED LEVEL OUTCOMES

A: Knowledge and understanding This programme/level provides opportunities for students to develop and demonstrate knowledge and understanding of*:*	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
A1 Principles and techniques of networks and cyber security-based research **A2** Enabling technologies for network and cyber security applications A4 The management and development of IT solutions to address networks and cyber security or other problems; A5 The professional, legal & ethical responsibilities of network and cyber security personnel within the organisational, technical and global contexts in which networks and cyber security are applied.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (A1, A2, A4, A5); • seminars (A1, A2, A4, A5); • directed reading (A1, A2, A4, A5); • use of the VLE (A1, A2, A4, A5);
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (A1, A2, A4, A5); • coursework essays/presentations (A1, A2, A4, A5); • coursework design and/or implementation (A1, A2, A4, A5).
B: Intellectual skills This programme/level provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
B1 Critically thinking, problem-solving and decision-making to solve complex networks and cyber security	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (B1, B2, B3, B5);

© Bournemouth University 2022

problems; B2 Analyse, interpret, synthesise and critically evaluate information from current research; B3 Critically evaluate and justify alternative approaches to solutions development; B5 Communicate findings to professional and academic standards.	• seminars (B1, B2, B3, B5); • directed reading (B1, B2, B3, B5); • use of the VLE (B1, B2, B3, B5). Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (B1, B2, B3, B5); • coursework essays/presentations (B1, B2, B3, B5).
C: Practical skills This programme/level provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
C1 Retrieve, select and evaluate information from a variety of sources ; C3 Select appropriate methods and tools for solving networks and cyber security problems; C4 Plan, monitor and evaluate the progress of a network and cyber security solution	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (C1, C3, C4); • seminars (C1, C3, C4); • directed reading (C1, C3, C4); • group exercises (C1, C3, C4). Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (C1, C3, C4); • coursework (C1, C3, C4);
D: Transferable skills This programme/level provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
D1 Demonstrate problem solving skills and the application of knowledge across the discipline areas. D2 Gather, select, and analyse a range of experimental and fieldwork data and present professionally using appropriate media.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (D1 – D4); • seminars (D1 – D4);

© Bournemouth University 2022

D3 Structure and communicate ideas professionally and effectively to appropriate professional and academic standards. D4 Demonstrate initiative, self direction and exercise personal responsibility for management of own learning.	• use of the VLE (D1 – D4); • directed reading (D1- D4).
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework essays/presentations (D1 – D4); • coursework design and implementation (D1 – D4).

LEVEL 4/Cert HE INTENDED LEVEL OUTCOMES

A: Knowledge and understanding This programme/level provides opportunities for students to develop and demonstrate knowledge and understanding of*:*	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
A1 Principles and techniques of networks and cyber security-based research A4 The management and development of IT solutions to address networks and cyber security or other problems; A5 The professional, legal & ethical responsibilities of network and cyber security personnel within the organisational, technical and global contexts in which networks and cyber security are applied.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (A1, A4, A5); • seminars (A1, A4, A5); • directed reading (A1, A4, A5); • use of the VLE (A1, A4, A5);
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (A1, A4, A5); • coursework essays (A1, A4, A5); • coursework design and implementation (A1, A4, A5)
B: Intellectual skills This programme/level provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:

© Bournemouth University 2022

B0 Critically thinking, problem-solving and decision-making to solve complex networks and cyber security problems; **B1** Analyse, interpret, synthesise and critically evaluate information from current research; B5 Communicate findings to professional and academic standards.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (B1, B2, B5); • seminars (B1, B2, B5); • directed reading (B1, B2, B5); • use of the VLE (B1, B2, B5);
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (B1, B2, B5); • coursework essays (B1, B2, B5); • coursework design and implementation (B1, B2, B5)
C: Practical skills This programme/level provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
C1 Retrieve, select and evaluate information from a variety of sources ; C4 Plan, monitor and evaluate the progress of a network and cyber security solution	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (C1, C4); • seminars (C1, C4); • group exercises (C4).
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework design and implementation (C1, C4); • Reflection (C1, C4).
D: Transferable skills This programme/level provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:

© Bournemouth University 2022

<table>
<tr>
<td rowspan="2">D2 Gather, select, and analyse a range of experimental and fieldwork data and present professionally using appropriate media.
D3 Structure and communicate ideas professionally and effectively to appropriate professional and academic standards.
D4 Demonstrate initiative, self direction and exercise personal responsibility for management of own learning.</td>
<td>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):

• lectures (D2 – D4);

• seminars (D2 – D4);

• use of the VLE (D2 – D4);

• directed reading (D2 – D4).</td>
</tr>
<tr>
<td>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):

• coursework essays (D2 – D4);

• examinations (D2 – D4);

• presentations (D2 – D4).</td>
</tr>
</table>

© Bournemouth University 2022

Programme Skills Matrix

Units		Programme Intended Learning Outcomes																		
		A 1	A 2	A 3	A 4	A 5	B 1	B 2	B 3	B 4	B 5	C 1	C 2	C 3	C 4	D 1	D 2	D 3	D 4	D 5
LEVEL 6	Internet and Wide Area Networks	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Human Computer Interaction	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Deep Learning and Applications	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Software Quality Assurance	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Digital Innovation and Transformation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Data Visualisation and Storytelling	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Individual Project	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Digital Futures (Elective)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
LEVEL 5	Communications and Networking	X	X		X	X	X	X	X		X	X		X	X	X	X	X	X	
	Security Operations (SecOps)	X	X		X	X	X	X	X		X	X		X	X	X	X	X	X	
	Software Engineering	X	X		X	X	X	X	X		X	X		X	X	X	X	X	X	
	Technological Innovations in Cyber Security	X	X		X	X	X	X	X		X	X		X	X	X	X	X	X	
	Network and Cyber Management	X	X		X	X	X	X	X		X	X		X	X	X	X	X	X	
	Software Business (Elective)	X	X		X	X	X	X	X		X	X		X	X	X	X	X	X	
LEVEL 4	Computer Fundamentals	X			X	X		X			X	X			X		X	X	X	
	Programming	X			X			X			X	X			X		X	X	X	
	Mathematics for Computing	X						X			X	X			X		X	X	X	
	Network Essentials	X			X	X		X			X	X			X		X	X	X	
	Introduction to Cyber Security	X			X	X		X			X	X			X		X	X	X	
	Computing and Society (Elective)	X			X	X		X			X	X			X		X	X	X	

© Bournemouth University 2022

Programme Specification - Section 2

A – Subject Knowledge and Understanding

This programme provides opportunities for students to develop and demonstrate knowledge and understanding of:

1. Principles and techniques of networks and cyber security-based concept
2. Enabling technologies for network and cyber security applications
3. A rigorous engineering approach to investigating and solving networks and cyber security problems such as those in the Internet, enterprise networks, cyber physical systems contexts;
4. The management and development of IT solutions to address networks and cyber security or other problems;
5. The professional, legal & ethical responsibilities of network and cyber security personnel within the organisational, technical and global contexts in which networks and cyber security are applied.

B – Intellectual Skills

This programme provides opportunities for students to:

1. Critically thinking, problem-solving and decision-making to solve complex networks and cyber security problems;
2. Analyse, interpret, synthesise and critically evaluate information from current research;
3. Critically evaluate and justify alternative approaches to solutions development;
4. Formulate, plan, execute, and report on a networks and cyber security project involving original contributions;
5. Communicate findings to professional and academic standards.

C – Subject-specific/Practical Skills

This programme provides opportunities for students to:

1. Retrieve, select and evaluate information from a variety of sources ;
2. Analyse, specify, design and implement networks and cyber security applications to meet business goals;
3. Select appropriate methods and tools for solving networks and cyber security problems;
4. Plan, monitor and evaluate the progress of a network and cyber security solution.

D – Transferable Skills

This programme provides opportunities for students to:

1. Demonstrate problem solving skills and the application of knowledge across the discipline areas.
2. Gather, select, and analyse a range of experimental and fieldwork data and present professionally using appropriate media.
3. Structure and communicate ideas professionally and effectively to appropriate professional and academic standards.
4. Demonstrate initiative, self direction and exercise personal responsibility for management of own learning.
5. Distil, synthesise and critically analyse alternative approaches and methodologies to problems and research results reported in literature and elsewhere.

© Bournemouth University 2022

ADMISSION REGULATIONS

The regulations for this programme are Bournemouth University's Standard Undergraduate Admission Regulations. Link to Admission Regulations

PROGRESSION ROUTES

Partnership arrangements provide formally approved progression routes through which students are eligible to apply for a place on a programme leading to a BU award. Please find information on Global Partnerships here: Global partnerships | Bournemouth University

ASSESSMENT REGULATIONS

The regulations for this programme are Bournemouth University's Standard Undergraduate Assessment Regulations.

WORK BASED LEARNING (WBL) AND PLACEMENT ELEMENTS

Students, under the guidance of lecturers and the Placement Office, are required to complete a sandwich year with a 30 week minimum placement requirement before Level 6.

The placement is assessed on a pass/fail basis using the log book and employer appraisal. The 30 week sandwich placement must be completed between Levels 5 and 6 and is a requirement for progression to Level 6 for the successful completion of the sandwich mode award.

Placement draws on some or all of the units studied on the first two levels of the programme. It provides the opportunity for the student to develop their abilities and understanding of software engineering related subjects, as well as providing a platform for successful entry into the profession following graduation. It applies and develops understanding and skills acquired in Levels 4 and 5, makes a major contribution to the understanding of the final level units, further develops final projects or dissertation research by utilising the context of the work experience as appropriate and enhances students' prospects of future employment.

© Bournemouth University 2022