Programme specification

1. Overview/ factual information

Programme/award title(s)	BSc (Hons) Cyber Security
Teaching Institution	Leeds City College
Awarding Institution	The Open University (OU)
Date of first OU validation	2017
Date of latest OU (re)validation	2022
Next revalidation	2027/8
Credit points for the award	120 for BSc (Hons)
UCAS Code	8H24
HECoS Code	100376
Programme start date and cycle of starts if appropriate.	September 2022
Underpinning QAA subject benchmark(s)	Computing 2019
Other external and internal reference points used to inform programme outcomes. For apprenticeships, the standard or framework against which it will be delivered.	UK Quality Code for Higher Education (2018) **Occupational Standard** TECIS600201 Identify cyber security threats and vulnerabilities https://www.ukstandards.org.uk/PublishedNos/Identify-cyber-security-threats-and-vulnerabilities-TECIS600201.pdf
Professional/statutory recognition	None
For apprenticeships fully or partially integrated Assessment.	n/a
Mode(s) of Study (PT, FT, DL, Mix of DL & Face-to-Face) Apprenticeship	*Full-Time and Part-Time*
Duration of the programme for each mode of study	1 year Full-Time 2 years Part-time

Dual accreditation (if applicable)	n/a
Date of production/revision of this specification	October 2021

Please note: This specification provides a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if s/he takes full advantage of the learning opportunities that are provided.

More detailed information on the learning outcomes, content, and teaching, learning and assessment methods of each module can be found in student module guide(s) and the students handbook.

The accuracy of the information contained in this document is reviewed by the University and may be verified by the Quality Assurance Agency for Higher Education.

2.1 Educational aims and objectives

The overall aims of the programme are to:

- Provide a comprehensive and challenging vocational programme in Cyber Security, including core and specialist modules, which facilitate access and progression for a wide range of students from diverse backgrounds into various computer/digital industry contexts.
- Offer a robust Top-up Degree programme that is relevant to current practice in the Cyber Security industry.
- Provide the opportunity for level 5 students to complete a full degree in the specialist field of Cyber Security
- Produce graduates who have the ability to critically reflect and learn from their practical and academic experience in a computing context and relate this experience to relevant theory.
- Produce highly motivated individuals who have the awareness, understanding and flexibility to continually redevelop their knowledge and skills.
- Produce graduates who have both subject specific skills (expressive, creative, technical) and transferable skills (communication, teamwork, project management) which are key to being employable within the cyber security industry.
- Produce graduates with autonomous and entrepreneurial abilities relevant to the cyber security.
- Produce graduates who have an analytical and reflective understanding of cyber security and wider digital subjects in the context of the workplace today and in relation to the wider social and cultural environment.
- Provide a supportive pastoral environment
- Provide opportunities to develop wider professional/soft skills
- Developing discipline and personal transferable skills so that during studies students may move directly into the cyber security industry

2.2 Relationship to other programmes and awards

(Where the award is part of a hierarchy of awards/programmes, this section describes the articulation between them, opportunities for progression upon completion of the programme, and arrangements for bridging modules or induction)

The BSc (Hons) programme provides an internal progression opportunity for students on our Foundation Degree in Cyber Security.

We would also accept external applicants who have level 5 qualifications such as Foundation Degrees, HNDs, or Diplomas of Higher Education in relevant subjects.

Our Foundation Degree in Cyber Security includes modules such as Linux and Scripting, Computer Forensics, Ethics and Ethical Hacking, and Securing Networks, as well as Employability Skills and a project driven module. Students joining the top-up course should have studied a variety of computing focused modules at level 5.

Students will be assessed on their skills and experience during the application/interview process.

The level 6 induction sessions and the supportive design of initial modules such as Research Methods will ensure students progressing from other level 5 qualifications will encounter a smooth transition to level 6.

Completion of this Top-Up will support progression to Masters programmes.

The Top-Up has been designed to provide students with the skills needed to work in the digital industry, either employed or as a freelance practitioner.

The three Top-Up programmes: Computer Science, Software Development and Cyber Security share some common modules. These modules are Research Methods, Digital Entrepreneurship and Major Project. These modular relationships will enable students to choose to work across the different disciplines within the three distinct topic areas. This approach will enable students, who wish to undertake a project in a different area to develop a primary skill (Software, Cyber Security or Computer Science) and potential to develop a secondary skill in a different area. This will not only broaden the skill are but also expand the nature of the student portfolio with the potential to increase employability options.

2.3 For Foundation Degrees, please list where the 60 credit work-related learning takes place. For apprenticeships an articulation of how the work based learning and academic content are organised with the award.
N/A

2.4 List of all exit awards
BSc. (Hons) Cyber Security – 120 credits BSc Cyber Security - 60 credits (any three 20-credit modules. This does not include the 40-credit *Undergraduate Major Project*)

3. Programme structure and learning outcomes

Programme Structure - LEVEL 6			
Compulsory modules	**Credit points**	**Is module compensatable?**	**Semester runs in**
Research Methods	20	Y	1
Cyber Security Incident Management	20	Y	1
Penetration Testing	20	Y	2
Digital Entrepreneurship	20	Y	2
Major Project	40	N	1 + 2
Additional modules			
Information Security Management	20	Y	1
Emerging Technologies	20	Y	2

Additional Modules

Two additional modules have been proposed and outlined. The learning outcomes of Information Security Management map to those of the Cyber Security Incident Management, and the learning outcomes of Emerging Technologies map to those of the Penetration Testing (one outcome does not map across but this is duplicated in the major project. The intention is that one of these additional modules can be swapped with one of the compulsory modules in the future if the operational demands of the course or employer request requires this.

Full Time Route

Over two days per week for one year. The major project is across both semesters. Research Methods is delivered alongside the Major Project during the first semester allowing students to develop the appropriate research skills at the foundation stage of the project.

Level 6			
Semester One	**Research Methods** (20 Credits)	**Cyber Security Incident Management** (20 Credits)	**Major Project** (40 Credits)
Semester Two	**Digital Entrepreneurship** (20 Credits)	**Penetration Testing** (20 Credits)	

Part Time Route

The part time programme is delivered over one day per week for two years. students will study either one or two modules per semester and the programme is designed to synchronise with the full-time provision. The major project is across both semesters of the second year and Research Methods is delivered alongside the Major Project during the third semester allowing students to develop the appropriate research skills at the foundation stage of the project.

Level 6		
Semester One		**Cyber Security Incident Management** (20 Credits)
Semester Two	**Digital Entrepreneurship** (20 Credits)	**Penetration Testing** (20 Credits)
Semester Three	**Research Methods** (20 Credits)	**Major Project** (40 Credits)
Semester Four		

Intended learning outcomes at Level 6 are listed below:

Learning Outcomes – LEVEL 6	
3A. Knowledge and understanding	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
K1 Concisely define and appraise the relevant theories, concepts and principles applicable to cyber security. K2 Demonstrate in-depth knowledge of a range of cyber security techniques. K3 Comprehensively describe the impact of ethical and legal issues relevant to cyber security K4 Identify and relate key aspects of the development of a major, specialist computing project to academic theory.	**Key Learning and Teaching Strategy Methods** The programme will place strong emphasis on providing a solid practical experience which will enhance and embed theoretical knowledge allowing learners to develop valuable skills in addition to confident understanding. These practical skills development and lecture experiences will be supported by workshops and problem-based classes with provision of on-line guided learning and self-assessment. Subject-specific VLE areas hosted on the Google platform and also offer extension and support materials which can be accessed at any time by students with an internet connection. Students will use reflective activities for learning and development of advanced practical skills, such as experimental design and planning Group and individual presentations will be used to strengthen student learning and to provide a basis for industry-style assessment, developing employability skills. Lectures and seminars will include specialised speakers with research experience and invited industry specialists. **Key Assessment Strategy/Methods** Each module has both formative and summative assessment including early assessment to support transition

Learning Outcomes – LEVEL 6	
3A. Knowledge and understanding	
	All modules have assessment which divides the learning outcomes between two tasks so that achievement is balanced over two forms of assessment. All outcomes are assessed in a summative manner but supported with formative work in preparation such as practice questions or online quizzes or practical skills audits. Assessment guidelines have been followed in terms of the amount and extent of assessment with detailed attention to the workload that each piece places on the student. A variety of practical assessment methods are used including computer application practical, design exercises, programming exercises that work to provide a good experience in preparation for employment. A variety of theoretical assessment methods are used including oral presentations, written assessments - including technical reports, literature searches and surveys, presentations and essays. These methods will also place an emphasis on developing soft skills identified by employers. Feedback is delivered in a variety of ways including, written, online and verbal within appropriate time scales (immediate during laboratory work, moderated and within three weeks for summative work). Design of assessment wherever possible offers an experience similar to a possible work-based scenarios in industry.

3B. Cognitive skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
C1 Synthesise and evaluate data/evidence from appropriate sources to make independent recommendations. C2 Demonstrate openness to adopting new ideas, concepts and techniques pertinent to practices in cyber security. C3 Apply detailed knowledge of appropriate cyber security tools and methods in defining complex problem. C4 Use supported rationale to challenge interpretations of current practice in cyber security.	Various methods and strategies of theoretical assessment methods will be to develop and assess the developemnt of the required outcomes. These will include oral presentations, written assessments - including technical reports, literature searches,surveys, and presentations. Practical methods will also be used including practical application of tools, application development, design exercises, and programming exercises.

3C. Practical and professional skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
P1 Demonstrate advanced cyber security skills. P2 Develop relevant solutions to complex cyber security problems. P3 Select and use appropriate cyber security techniques. P4 Employ a range of recognised frameworks when developing a cyber security solution.	Assessment methods will include practical application design and development, appropriate application of tools, methods and techniques. Learning strategies will include lectures, presentations, reports, practical workshops and demonstrations.

3D. Key/transferable skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
T1 Communicate clearly, fluently and effectively in a range of styles appropriate to the context. T2 Able to act autonomously with limited supervision or direction within agreed guidelines. T3 Select and apply appropriate numerical and statistical methods. T4 Demonstrate creativity, innovation and independent thinking.	Various methods and strategies of learning and assessment will be employed to develop and assess the development of the required outcomes. These will include presentations, written assessments - including technical reports, literature searches,surveys, and oral presentations.

Learning Outcomes BSc. (Hons) Cyber Security
By the end of the programme successful students will have demonstrated all of the above learning outcomes.

Learning Outcomes BSc Cyber Security
By the end of the programme, students awarded Ordinary degrees will have demonstrated the majority of the above learning outcomes (approximately 13 out of 16). However, these students will have gained fewer credits at Level 6 than students awarded a Honours degree as they only need 60 credits from modules other than the Dissertation to achieve the level. In most cases, their knowledge will typically be less broad and will typically be less proficient in higher-level skills.

4. Distinctive features of the programme structure

- **Where applicable, this section provides details on distinctive featurs such as:**
- where in the structure above a professional/placement year fits in and how it may affect progression
- any restrictions regarding the availability of elective modules
- where in the programme structure students must make a choice of pathway/route
- **Additional considerations for apprenticeships:**
- how the delivery of the academic award fits in with the wider apprenticeship
- the integration of the 'on the job' and 'off the job' training
- how the academic award fits within the assessment of the apprenticeship

The newly formed STEM department is uniquely positioned to offer excellent opportunities to students on our programmes. The provision in the department includes Computing, Computer Games, Engineering and Science programmes. This pack of courses offers exciting opportunities for collaborative work between students and staff.

The cross over between the different disciplines outlined are numerous. The aim of the programmes is to have cross collaboration across all levels. Examples of the opportunities are to have Computing students who will have computer programming skills to work with game development students who will have 3D modelling and game level design skills, the potential outcomes are fully working prototype games, with the backend programming carried out by computing students.

Cyber Security students can potentially work with software development students to develop secure systems in a range of commercial contexts.

The Engineering industry are requiring more digital skills in manufacturing, automation and 3D product visualisations. Computing tutors are fully skilled in the topics of 3D modelling and could port these skills into Computer Aided Design. Engineering staff could deliver Maths and Science based topics to Cyber Security students to add further context to their studies by developing a broad range of skills and knowledge in STEM subjects.

These staff skills and knowledge place the department in a unique position to deliver modern programmes that are reflective of industry needs and practices.

All STEM courses are delivered on two floors with teaching spaces that will easily facilitate collaborative opportunities.

The focus of the programme is preparing students for a career in the cyber security and digital sector, either as a self-employed practitioner or as an employee of an SME or large-scale company. There is an overall emphasis on work related learning that reflects industry practice. Work related progression is the focus of two modules (Digital Entrepreneurship and Major Project) with the aim of developing professionalism and preparing graduates for the world of employment in the sector.

The institution currently offers computing and digital related studies from Level 1 to level 6, this unique feature, supports students who develop better in a familiar environment with staff they know, helping them to achieve their full potential in a supportive environment.

A focus of the programme is the development of practical skills that will form the foundation of a varied portfolio. Skills that are in demand and will demonstrate practical experience to employers.

There is also a focus on developing personal and employability skills that are fast becoming a requirement of digital and tech employers in addition to practical skills. These skills often termed as “soft Skills” are embedded in the programme.

The department has a good working relationship with the institution’s internal department, who have provided advice and guidance on module content. This includes a dedicated IT technician who oversees the IT equipment of these courses.

The luminate internal departments are open to providing top-up year students with the opportunity of short-term voluntary work experience.

This is not a requirement of the course in terms of assessment and achievement but is encouraged if students have the time to fit work experience around course, home and personal commitments.

5. Support for students and their learning.
(For apprenticeships this should include details of how student learning is supported in the work place)

The award adopts the following approach to student learning support.

Tailored induction to support the transition to Higher Education

A robust communications system functions to give students access to lecturers and management; this includes e-mail, the VLE and notice boards and open office culture.

All necessary information about the programme is provided by means of the student handbook, module handbooks and the VLE.

Each student is allocated a personal tutor for regular tutorials and personal development planning. This is implemented in the first term and continued throughout the year of study.

Practical work supported by regular peer feedback through workshop critiques.

Shared documents and folders between staff and students to support live editing and feedback on work.

There is an extensive range of learning resources in the library, supported by specialist staff that provide bespoke study skills sessions for students.

The University Centre provides an extensive range of services for students, including support for those with special needs, welfare, counselling, financial and careers advice

Students will be given a Chromebook or an equivalently priced laptop if they prefer when they start the course. There will be an option for students to upgrade this to a more powerful laptop if they agree to pay a supplement that will make up the difference in the cost of a Chromebook and the more powerful laptop. This cost will be reviewed yearly to reflect the changes in cost of devices year on year. The Chromebook or laptop will be required to last students the full duration of the course.

The department has a coaching tutor employed to support students and their learning. The coaching tutor will provide support in academic, technical and personal settings. The coaching tutor will also support students with deadlines, applying for short extension and mitigation and will also track and chase low attendance and engagement.

Personal and academic tutorials will be carried out by the course team, these meetings will provide regular one to one support. Discussions will be logged and shared with module tutors to identify potential problems but to also highlight and share praise for excellent performance on module tasks.

The coaching tutor will act as the go to person for support. This will provide consistency for students with a clearly support staff who will get to know the students and their individual support needs.

6. Criteria for admission
(For apprenticeships this should include details of how the criteria will be used with employers who will be recruiting apprentices.)

Admission Criteria		
	Typical offer	**Minimum Offer**
Foundation Degree/HND:	A typical offer is likely to be a Pass at Foundation Degree or a Pass grade on a relevant HND,	A minimum offer is a Pass average at Foundation Degree or a Pass grade on a relevant HND,
IELTS:	IELTS 6.0 with no less than 5.5 in any component.	
International qualifications:	International qualifications will be assessed against these criteria	
Mature applicants:	University Centre Leeds welcomes applications from mature* applicants who may not have met the academic criteria, but who can demonstrate a wealth of experience in their chosen field. Candidates in this category and otherwise are likely to be interviewed to assess their suitability for the course and may be asked to provide a portfolio of evidence to support their application. **21 years and over at the start of the course*	
RPL claims:	The course structure actively supports claims for Recognition of Prior Certified Learning (RPL).	

7. Language of study

English

8. Information about non-OU standard assessment regulations (including PSRB requirements)

N/A

9. For apprenticeships in England End Point Assessment (EPA). *(Summary of the approved assessment plan and how the academic award fits within this and the EPA)*
N/A

10. Methods for evaluating and improving the quality and standards of teaching and learning.
In addition to the Annual Programme Monitoring process the following mechanisms are in operation: ● Peer review ● Annual Planning ● Peer Observation ● Student module reviews ● Student voice ● Tutor module reviews ● Enrolment and induction reviews ● Course Committee meetings ● Pathway Committee meetings ● Student Pathway meeting ● Cross college quality and enhancement committee meeting ● Employer feedback

11. Changes made to the programme since last (re)validation
This validation has seen significant changes in the makeup of the modules and their content in comparison to the previous top-up courses ran by the Digital and Engineering team. The content of these new modules has been designed to follow on from the new Foundation Degree courses that have been recently validated. These are more focused along certain disciplines, Computer Science, Software Development and Cyber Security, rather than the broad nature of the previous course. This has seen an increase in the discipline specific modules at level 5 and resulting in more able students at the end of level 5 in their chosen discipline. The new modules will consist of two technical focused modules to further develop the discipline specific practical skills developed at levels 4 and 5. On the Cyber Security Top-up, course this will consist of Cyber Security Management and Penetration Testing modules building on the security focused modules from level 5. This has allowed these new modules to be more in depth and further enhance these specialised practical skills while at the same time further develop problem-solving and organisational skills as well as developing new career specific professional skills. Each of these discipline specific modules has pre-requisite entry information to ensure students have the correct pre-existing technical skills at the start of the module to be able to work at or near the expected level. Alongside the two discipline-specific technical modules, each course will consist of three common modules. The Research Skills module has been renamed Research Methods and although the content has the remained virtually the same the assessment has changed significantly to remove some of the dependency on the existing project module. The previous literature review assessment has now been incorporated into the Major Project module and been

replaced by a research portfolio where students will demonstrate a range of research methods. The existing presentation of a proposal for the final year project has remained. A new and innovative Digital Entrepreneurship module will develop new skills in students relating to how entrepreneurial ventures can be developed using digital technology and e-marketing.
The 40-credit Project module has been renamed Major Project and based on the advice from the current external examiner and academic reviewer the emphasis of the module has changed focus from a research focus to a joint practical and research/essay outcome.

The existing Project Management module has been removed and much of its content moved into the new Major Project module. The new module will consist of two assessments. Task 1, design, practical work, and testing. Task 2, project report with a literature review, methods, outcomes, discussion, and conclusions.

Annexe 1: Curriculum map

Annexe 2: Teaching and Learning Map

Annexe 3: Assessment Map

Annexe 4: Curriculum mapping against the apprenticeship standard or framework (delete if not required.)

Annexe 5: Notes on completing the OU programme specification template

Annexe 1 - Curriculum map

This table indicates which study units assume responsibility for delivering (shaded) and assessing (ü) particular programme learning outcomes.

BSc (Hons) Cyber Security																	
Level	**Study module/unit**	**Programme outcomes**															
		K1	**K2**	**K3**	**K4**	**C1**	**C2**	**C3**	**C4**	**P1**	**P2**	**P3**	**P4**	**T1**	**T2**	**T3**	**T4**
6	Research Methods	✓					✓		✓					✓		✓	
	Cyber Security Incident Management		✓					✓				✓	✓		✓		
	Penetration Testing		✓		✓			✓		✓	✓						
	Digital Entrepreneurship			✓		✓	✓					✓		✓			✓
	Major Project	✓		✓	✓	✓			✓	✓	✓		✓		✓	✓	✓
	Information Security Management (Swappable with Cyber Security Incident Management)		✓					✓				✓	✓		✓		
	Emerging Technologies (Swappable with Penetration Testing)		✓		✓			✓			✓	✓	✓				

BSc Cyber Security																	
Level	**Study module/unit**	**Programme outcomes**															
		K1	**K2**	**K3**	**K4**	**C1**	**C2**	**C3**	**C4**	**P1**	**P2**	**P3**	**P4**	**T1**	**T2**	**T3**	**T4**
6	Research Methods	✓					✓		✓					✓		✓	
	Cyber Security Incident Management		✓					✓				✓	✓		✓		
	Penetration Testing		✓		✓			✓		✓	✓						
	Digital Entrepreneurship			✓		✓	✓					✓		✓			✓

	Learners must complete three of the four modules above in order to achieve the exit award.																
	Information Security Management (Swappable with Cyber Security Incident Management)		✓					✓				✓	✓		✓		
	Emerging Technologies (Swappable with Penetration Testing)		✓		✓			✓			✓	✓	✓				

Annexe 2 – Teaching and Learning Map

BSc (Hons) Cyber Security

	Methods								
Module Titles	Lectures	Student led/ interactive/ shared learning seminars	Case Studies	Skills workshops	Practicals (design and production sessions)	Group activities	Guest speakers	Independent / E Learning/ On-line forums	(insert other)
Research Methods	✔	✔					✔	✔	
Digital Entrepreneurship	✔	✔	✔			✔		✔	
Major Project	✔	✔			✔			✔	
Cyber Security Incident Management	✔	✔	✔	✔	✔			✔	
Penetration Testing	✔	✔	✔	✔	✔			✔	

BSc Cyber Security

	Methods								
Module Titles	Lectures	Student led/ interactive/ shared learning seminars	Case Studies	Skills workshops	Practicals (design and production sessions)	Group activities	Guest speakers	Independent / E Learning/ On-line forums	(insert other)
Research Methods	✔	✔					✔	✔	
Digital Entrepreneurship	✔	✔	✔			✔		✔	

Cyber Security Incident Management	✔	✔	✔	✔	✔			✔	
Penetration Testing	✔	✔	✔	✔	✔			✔	
Learners must complete three of the four modules above in order to achieve the exit award.									

Annexe 3 – Assessment Map

Please provide a map for each named pathway or separate award. Adjust assessment methods across the top of each column to suit your programme needs, adding in additional columns where necessary, insert module titles in the left of the grid and indicate which methods will be used in each module, detailing the weighting of the task, word count (or equivalent), and submission week. Please ensure you provide a good and appropriate mix of methods. Additional maps can be added for different delivery models, e.g. Apprenticeships.

Level 6

	Methods								
Module Titles	Report	Proposal	Feasibility Study	Digital Product	E-Portfolio	Evaluation	Designs portfolio	Practical portfolio	Presentation
Research Methods					60% (3000 words) week 10				40% (16 mins) week 14
Digital Entrepreneurship			40% (2000 words) week 22	60% (15 mins presentation & product) week 28					
Major Project	60% (7000 words) week 30 Inc (1500 words proposal) Check point for proposal week 8						40% (3000 words eq) week 26		
Cyber Security Incident Management	60% (3000 words) week 12							40% (2000 words eq) week 15	
Penetration Testing								60% (3000 words eq) week 29	40% (2000 words eq) week 24

Information Security Management	60% (3000 words) week 12							40% (2000 words eq) week 15	
Emerging Technologies	30% (1500 words) week 23							70% (3500 words eq) week 29	

Annexe 5: Notes on completing programme specification templates

1 **-** This programme specification should be mapped against the learning outcomes detailed in module specifications.

2 – The expectations regarding student achievement and attributes described by the learning outcome in section 3 must be appropriate to the level of the award within the **QAA frameworks for HE qualifications**: http://www.qaa.ac.uk/AssuringStandardsAndQuality/Pages/default.aspx

3 – Learning outcomes must also reflect the detailed statements of graduate attributes set out in **QAA subject benchmark statements** that are relevant to the programme/award: http://www.qaa.ac.uk/AssuringStandardsAndQuality/subject-guidance/Pages/Subject-benchmark-statements.aspx

4 – In section 3, the learning and teaching methods deployed should enable the achievement of the full range of intended learning outcomes. Similarly, the choice of assessment methods in section 3 should enable students to demonstrate the achievement of related learning outcomes. Overall, assessment should cover the full range of learning outcomes.

5 - Where the programme contains validated **exit awards** (e.g. CertHE, DipHE, PGDip), learning outcomes must be clearly specified for each award.

6 - For programmes with distinctive study **routes or pathways** the specific rationale and learning outcomes for each route must be provided.

7 – Validated programmes delivered in **languages other then English** must have programme specifications both in English and the language of delivery.