Leeds Trinity University

Programme Specification

With effect from: **September 2024**

A programme specification is the definitive record of your programme of study at the University. It sets out the aims, learning outcomes, and indicative content of the programme. You should read this programme specification alongside the relevant module descriptors and the University's Taught Programme Academic Regulations.

This specification only applies to the delivery of the programme indicated below. The details in this specification are subject to change through the modifications or periodic review processes.

1 Programme name and award

This programme specification relates to the following award(s)
BSc (Hons) Computer Science with Cyber Security

2 Aims of the programme

Rationale and general aims, including what is special about this programme
The BSc (Hons) Computer Science with Cyber Security programme readies you for a rapidly evolving sector. It encompasses traditional computer science and cyber security principles within the framework of adaptable and dynamic work environments. Given Leeds's prominence as a tech hub, the programme is crafted in collaboration with local providers, ensuring a strong emphasis on current and future developments and the preparation of highly employable graduates. The programme aims are to: • Foster a solid knowledge base in the core areas of computer science and cyber security for diverse professional roles. • Instil understanding and practical experience of the latest developments in software technologies, programming concepts and commercial work practices and methods. • Cultivate an understanding of project-based work in a dynamic and ever-changing cyber security environment, emphasising skills that empower graduates to excel in such contexts. • Develop critical and independent thinking skills, whether working as an individual or collaboratively within a team.

- Develop a range of transferable skills relevant to graduate-level employment, gained through academic projects and professional placements.

3 Level Learning Outcomes and Attributes and Skills or Employability Outcomes

Learning outcomes are expressed in terms of:

- Knowledge and understanding (K)
- Intellectual / cognitive / 'thinking' skills (I)
- Practical skills specific to the subject (P)
- Attributes and Skills (undergraduate) (AS)

We design assessment tasks to enable you to demonstrate the Level Learning Outcomes and relevant Employability Outcomes for your level of study. To a greater or lesser extent, all Level Learning Outcomes at each level of your study are embedded in the assessment task(s) at that level. This means we can take a more integrated view of your overall performance at a level.

To progress to the next level, or to receive an award, you will need to satisfy the Level Learning Outcomes below and relevant Attributes and Skills Outcomes (UG) or Employability Outcomes (PG) and achieve credit as per the Taught Programme Academic Regulations.

Level Learning Outcomes	
Level 4	
K1	**Subject knowledge** - knowledge and understanding of the subject of computing and computer applications. This includes relevant academic and professional standards and commercial contexts as required to practise in the cyber security field.
K2	**Currency of knowledge** - knowledge and understanding of the latest technologies, methodologies and best practices in the field of computer science and cyber security.
K3	**Contextual knowledge** - knowledge of a range of issues (moral and ethical, legal, social, environmental and commercial) relevant to professional practice in computer science and cyber security.
K4	**Commercial understanding** - the ability to comprehend and apply business concepts and principles, understanding the broader economic, organisational and market context in which computing solutions are developed and deployed.
I1	**Problem-solving** - the ability to identify, use and justify problem-solving techniques to satisfy a set of given requirements, as an individual and within a team.
I2	**Investigation** - the ability to carry out investigations to support software development, including the specification, design and development processes.

I3	**Analytical perspective** - the ability to use appropriate strategies to tackle computing problems, guided by theoretical understanding of the subject area.
Level 5	
K1	**Subject knowledge** - a deep understanding of the technical aspects of computer science and cyber security, encompassing a broad range of topics and skills related to the design, development and implementation of computer systems, software and algorithms.
K2	**Currency of knowledge** - professional understanding of a range of standard and emergent technologies in breadth and depth, programming tools and methodologies, computational thinking and problem-solving strategies and techniques.
K3	**Contextual knowledge** - the application of coherent and detailed knowledge of a range of issues (moral and ethical, legal, social, environmental, and commercial) relevant to professional practice in the computer science and cyber security sector.
K4	**Commercial understanding** - proficiency in the comprehension and application of business concepts and principles, understanding the broader economic, organisational and market context in which computing solutions are developed and deployed.
I1	**Problem-solving** - the ability to critically analyse, strategise and implement effective solutions to complex challenges.
I2	**Investigation** - the ability to conduct investigations into the nature of software development, including the specification, design, and development processes.
I3	**Analytical perspective** - the application of appropriate strategies to tackle complex computing problems, guided by a theoretical understanding of the subject area.
Level 6	
K1	**Subject knowledge** - a comprehensive understanding and expertise in the technical aspects of computer science and cyber security, including relevant academic and professional standards and commercial contexts as required to practise in the computer science field.
K2	**Currency of knowledge** - critical and professional understanding and evaluation of a range of standard and emergent technologies, programming tools, methodologies and best practices in computer science and cyber security.
K3	**Contextual knowledge** - critical understanding and evaluation of a range of issues (moral and ethical, legal, social, environmental and commercial) relevant to professional practice in the subject specialism.

K4	**Commercial understanding** - a comprehensive understanding of the broader context in which technology is applied, recognising the needs, challenges and constraints to ensure that technology is effective and aligned with the goals and values of its environment.
I1	**Problem-solving** - the ability to critically evaluate and select problem-solving techniques to computing requirements, as an individual and within a team.
I2	**Investigation** - the ability to critically investigate software development including specification, design and secure development processes.
I3	**Analytical perspective** - a systematic and methodical approach to understanding and interpreting complex computing problems in order to make informed decisions, optimise solutions and address challenges effectively.

Attributes and Skills Outcomes (undergraduate)	
AS1	**Working Independently** - prioritising workload, anticipating and troubleshooting potential problems, and achieving this without requiring continual oversight from a supervisor or manager.
AS2	**Research & Thinking Critically** - systematic investigation of resources to identify relevant information. Critical thinking refers to a process of independent scrutiny, allowing formation of a well-reasoned opinion for application of the research to decision-making and action.
AS3	**Digital Confidence** - identifying, learning and confident adoption of digital tools, applications and software to improve existing processes, meet emerging challenges or develop new approaches.
AS4	**Adaptability** - the ability to make the most of changing circumstances and adapt to new conditions.
AS5	**Resilience** - the ability to recognise that you will be exposed to adversity but that you will be able to respond positively and ultimately adapt and grow from challenging events.
AS6	**Professional Outlook** - preparing yourself to successfully research, plan and apply for opportunities through effectively articulating your skills and attributes whilst understanding how to present yourself in professional working environments to achieve your career goals.
AS7	**Effective Communication** - the ability to work cooperatively with others to achieve a group objective and the recognition that good leadership empowers achievement of collective goals through combined efforts.
AS8	**Ethics, Diversity, Sustainability** - making a positive impact on society and the environment as a whole.
AS9	**Enterprise and Entrepreneurship** - entrepreneurship is the application of enterprise behaviours, attributes and competencies into the creation of cultural, social, or economic value. Enterprise is generating and applying ideas that are practical when undertaking a new venture or project.

4 External Benchmarks

Statement of congruence with the relevant external benchmarks
All Leeds Trinity University programmes are congruent with the Frameworks for HE Qualifications (FHEQ) and, where appropriate, the Qualifications and Credit Framework (QCF) (formerly National Qualification and Credit Framework (NQF)). The Computer Science with Cyber Security programme is congruent with the most recent QAA Benchmark Statement for Computing (2022). **For students studying at the Leeds Trinity campus**, accreditation by BCS, The Chartered Institute for IT, will be sought once the programme is established.

5 Indicative Content

Summary of content by theme
The BSc (Hons) Computer Science with Cyber Security programme empowers you to cultivate discipline-specific skills in software development, organisational processes, professional experience and collaborative professional project work. The curriculum employs vertical strands to foster skill and knowledge development in these areas throughout the three years of undergraduate study. This programme offers opportunities for gaining specialised skills and knowledge in emerging fields within the realm of cyber security. Throughout all levels, you will actively participate in collaborative professional project work, integrating content from all modules at each level. Core knowledge and skills acquired at each level contribute to collaborative practice, preparing you for professional experiences. The programme features a progressive and convergent structure, establishing core disciplines in the first year and synthesising them in the second year to ready you for project work in the final year. The capstone of the programme is the final year project module, surpassing a traditional final year project by necessitating continuous engagement with peers and an employer mentor. This module requires the application of practical and theoretical knowledge in a professional context, serving as a comprehensive integration of learning across previous modules.

6 Programme Structure

Programme Structure – BSc (Hons) Computer Science with Cyber Security			
Duration	3 years full-time		
Total credit rating	360 (180 ECTS)		
Level 4 – With effect from: September 2024			
Core: You are required to take the following modules			
Module Code	Module Title	Semester	Credits

COM4103	Software Development	1	30
COM4113	Tech Stack	1	30
COM4043	Computing Skills	2	30
*COM4143	User Experience	2	30
* Indicates Integrated Assessment			
Level 5 – With effect from: September 2025			
Core: You are required to take the following modules			
Module Code	Module Title	Semester	Credits
COM5313	Ethical Hacking	1	30
COM5113	Algorithms and Data Structures	1	30
COM5303	Computer Networking and Security	2	30
COM5043	Thematic Project	2	30
Level 6 – With effect from: September 2026			
Core: You are required to take the following modules			
Module Code	Module Title	Semester	Credits
COM6305	Secure Development and Deployment	1	15
COM6303	Cyber Security	1&2	30
COM6103	Data Science	1&2	30
COM6045	Project	1&2	45

7 Pre-requisites

Modules students must study and achieve credit for before enrolling on a module at a higher level, or attaining their final programme award
None.

8 Learning, Teaching and Assessment

The University's Learning, Teaching and Academic Experience Strategy informs the design of your programme. You can find more information about learning, teaching and assessment for your programme (including information on Integrated Assessment) within the relevant Assessment Handbooks.

9 Entry requirements

Do the University's standard entry requirements apply (as outlined within the University's Admissions Policy)?	Yes
Detail of any deviation from (or within) and/or addition to the University's standard entry requirements (if applicable), e.g. English Language and/or English Literature requirement	N/A

10 Additional support needs

Students with disabilities or other support needs are welcome and are expected to be able to participate fully in this programme. Arrangements will be made, via the normal University support systems, to accommodate students with additional support needs wherever possible, with reasonable adjustments made to accommodate individual needs.

Programme-specific requirements / unavoidable restrictions on participation in the programme
N/A

11 Technical Information

Awarding Body / Institution	Leeds Trinity University
Teaching Institution	Leeds Trinity University
Parent Faculty	Business, Computing and Digital Industries
Parent School	Computer Science
Professional accreditation body	**For students studying at the Leeds Trinity campus**, accreditation by BCS, The Chartered Institute for IT, will be sought once the programme is established.
Final award	BSc (Hons)
Title of programme(s)	Computer Science with Cyber Security

Subsidiary (fallback) award(s)	Certificate of Higher Education in Computer Science with Cyber Security Diploma of Higher Education in Computer Science with Cyber Security Ordinary Degree in Computer Science with Cyber Security
Honours type	Single
Duration and mode(s) of study	3 years full time
Month/year of approval of programme	February 2024
Periodic review due date	As scheduled
HECoS subject code(s)	100366 – computer science (67%) 100376 – computer and information security (33%)
UCAS course code(s)	COMPSCI
SITS route codes	COMPSCI / UGBSN
Delivery venue(s)	Horsforth Campus……. No City Campus……...Yes

12 Level Learning Outcomes and Employability Outcomes

The grids below demonstrate where Level Learning Outcomes and Attributes and Skills Outcomes or Employability Outcomes are assessed at module level and ensure that students are assessed in all Level Learning Outcomes at each level of their study. Students might not be assessed in all Attributes and Skills Outcomes at each level of study. However, all Attributes and Skills/Employability Outcomes will have been assessed by the end of the programme.

Level 4	**Assessed level learning outcomes**								**Skills development**								
	K1	**K2**	**K3**	**K4**	**I1**	**I2**	**I3**		**AS1**	**AS2**	**AS3**	**AS4**	**AS5**	**AS6**	**AS7**	**AS8**	**AS9**
Lighter or hatched shading indicates modules that are not core, ie. not all students on this programme will undertake these.	Subject Knowledge	Knowledge Currency	Contextual Knowledge	Commercial Understanding	Problem Solving	Investigation	Analytical Perspectives		Working Independently	Research and Thinking Critically	Digital Confidence	Adaptability	Resilience	Professional Outlook	Effective Communication	Ethics, Diversity, Sustainability	Enterprise and Entrepreneurship
COM4103 Software Development	■	■	■		■	■	■		■		■	■	■		■		■
COM4043 Computing Skills			■	■	■	■	■		■	■	■	■	■	■	■	■	
COM4113 Tech Stack	■	■			■	■	■		■		■	■	■		■		
*COM4143 User Experience	■	■	■	■	■	■	■		■	■	■	■	■	■	■		■

Level 5	Assessed level learning outcomes								Skills development								
	K1	K2	K3	K4	I1	I2	I3		AS1	AS2	AS3	AS4	AS5	AS6	AS7	AS8	AS9
Lighter or hatched shading indicates modules that are not core, ie. not all students on this programme will undertake these.	Subject Knowledge	Knowledge Currency	Contextual Knowledge	Commercial Understanding	Problem Solving	Investigation	Analytical Perspectives		Working Independently	Research and Thinking Critically	Digital Confidence	Adaptability	Resilience	Professional Outlook	Effective Communication	Ethics, Diversity, Sustainability	Enterprise and Entrepreneurship
COM5313 Ethical Hacking	■	■	■		■	■	■		■		■	■	■	■	■	■	
COM5303 Computer Networking and Security	■	■	■		■				■		■	■	■		■	■	
COM5113 Algorithms and Data Structures	■	■	■		■				■		■	■	■		■		
COM5043 Thematic Project	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■

Level 6	Assessed level learning outcomes								Skills development								
	K1	K2	K3	K4	I1	I2	I3		AS1	AS2	AS3	AS4	AS5	AS6	AS7	AS8	AS9
Lighter or hatched shading indicates modules that are not core, ie. not all students on this programme will undertake these.	Subject Knowledge	Knowledge Currency	Contextual Knowledge	Commercial Understanding	Problem Solving	Investigation	Analytical Perspectives		Working Independently	Research and Thinking Critically	Digital Confidence	Adaptability	Resilience	Professional Outlook	Effective Communication	Ethics, Diversity, Sustainability	Enterprise and Entrepreneurship
COM6303 Cyber Security	■	■	■		■	■	■		■	■	■	■	■	■	■	■	
COM6103 Data Science	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■
COM6305 Secure Development and Deployment	■	■	■		■				■	■	■	■	■	■		■	
COM6045 Project	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■