Programme Specification

Cyber Security [Frenchay]

Version: 2026-27, v2.0, Validated

Contents

Programme Specification 1

Section 1: Key Programme Details 2

Part A: Programme Information 2

Section 2: Programme Overview, Aims and Learning Outcomes 2

Part A: Programme Overview, Aims and Learning Outcomes 3

Part B: Programme Structure 9

Part C: Higher Education Achievement Record (HEAR) Synopsis 10

Part D: External Reference Points and Benchmarks 11

Part E: Regulations 12

Section 1: Key Programme Details

Part A: Programme Information

Programme title: Cyber Security [Frenchay]

Highest award: MSc Cyber Security

Interim award: PGCert Cyber Security

Interim award: PGDip Cyber Security

Awarding institution: UWE Bristol

Teaching institutions: UWE Bristol

Study abroad: No

Year abroad: No

Sandwich year: No

Credit recognition: No

School responsible for the programme: CATE School of Computing and Creative Technologies, College of Arts, Technology and Environment

Professional, statutory or regulatory bodies:

National Cyber Security Centre (NCSC)

Modes of delivery: Full-time, Part-time

Entry requirements: For the current entry requirements see the UWE public website.

For implementation from: 01 September 2026

Programme code: I90000

Section 2: Programme Overview, Aims and Learning Outcomes

Part A: Programme Overview, Aims and Learning Outcomes

Overview: This programme is aimed at graduates of computing based degrees; for example, Computer Science, Cyber Security, Information Security, who wish to develop their knowledge, understanding, and skills in the general aspects of Cyber Security. The programme will provide them with a common foundation, which then forms the basis for the study of various aspects and technologies of secure systems.

Graduates of this programme will typically have the appropriate knowledge and skills to undertake senior technical roles within Cyber Security.

We aspire to develop graduates who are technically proficient, ethically grounded, and strategically aware. Students will emerge as critical thinkers and problem-solvers, equipped to address complex security challenges across diverse sectors. They will demonstrate a strong understanding of cyber risk, governance, and emerging technologies, alongside practical skills in threat detection, mitigation, and secure system design. With a commitment to lifelong learning and professional integrity, graduates will be prepared to lead, innovate, and collaborate in shaping a secure digital future for organisations and society at large.

Features of the programme: NCSC-Certified Programme: This course is certified by the UK's National Cyber Security Centre (NCSC), ensuring it meets high standards in cyber security education and aligns with industry needs.

Professional Engagement: Students have the opportunity to engage with the UK Cyber Security Council, supporting professional development and alignment with national frameworks.

Industry and Academic Insights: Regular guest lectures feature speakers from leading organisations and universities, offering cutting-edge insights and real-world perspectives.

Career-Focused Development: Regular seminars are tailored to career progression, including CV clinics, mock interviews, and other employability-focused sessions.

Regular Research Meetings: Open to all staff and students, these sessions provide a platform to discuss ongoing research, explore new ideas, and collaborate on projects.

Educational Aims: The programme develops underpinning knowledge and skills in fundamental areas such as computer and network security and contemporary techniques. Emerging technologies are particularly relevant in cyber security as they are used when handling large amounts of data and also when running complex algorithms over significantly large data sets.

Students further develop their knowledge and skills, studying various aspects and technologies within the cyber security domain; for example: cryptography as applied to cyber security, the security of smart devices and critical systems.

Students will study information security management and information risk management (placing these within a legal context).

Additionally, students will develop their knowledge and understanding of current issues and research within the cyber security domain, and develop research skills in preparation for their final project. Within the final project, students will identify and research a topic relevant to the cyber security domain.

Programme Learning Outcomes:
On successful completion of this programme graduates will achieve the following learning outcomes.

Programme Learning Outcomes

PO1. Demonstrate and utilise deep systematic knowledge and understanding of the concepts and technologies used to establish and maintain computer and network security.

PO2. Demonstrate critical awareness of how contemporary methodological approaches and legal frameworks shape and influence the practice of information security management and information risk management.

PO3. Critically analyse the complexities of contemporary computer systems and synthesise the cyber security challenges they present.

PO4. Develop suitable and sustainable models and critical responses to examine cyber security issues and to identify future solutions.

PO5. Design and implement technical security solutions taking into account the current and emerging landscape of threats and vulnerabilities.

PO6. Communicate ideas, arguments and knowledge in a professional and effective manner through both individual and group work scenarios.

PO7. Demonstrate advanced practical, analytical, and research skills through well-defined empirical investigation, and critically disseminate outcomes to a professional audience as well as non-specialist audiences.

Assessment strategy: The programme adopts a practice-oriented, programme-level approach to assessment, designed to ensure students develop robust technical knowledge, proficiency with industry-relevant tools, and the ability to design and implement effective security measures while understanding adversarial behaviours. Assessment is aligned with the learning outcomes of each module and the programme as a whole, providing a clear link between the skills and knowledge gained and the professional capabilities required in the cyber security sector.

A variety of assessment types is employed to reflect both disciplinary and practice-oriented approaches, mirroring real-world cyber security scenarios. For example:

Portfolios of practical skills allow students to demonstrate hands-on technical competencies, proficiency in using industry-standard tools, and the ability to analyse and respond to complex security challenges.

Reports and applications assess students' ability to conduct structured analysis, articulate findings clearly, and propose and develop solutions or strategies in contexts that simulate workplace tasks.

Group projects and presentations foster teamwork, collaboration, and professional communication skills to disseminate findings to specialist and non-specialist audiences, while also encouraging critical analysis of risk and security management,

which are essential for functioning effectively in multidisciplinary teams.

In-class tests provide opportunities to evaluate knowledge under time-constrained conditions, ensuring students can apply theoretical concepts to practical scenarios.

Dissertation-style research develops enquiry-based learning and advanced research skills, critical thinking, and the ability to conduct independent, in-depth investigation aligned with both academic and industry standards.

This variety of assessment approaches is purposefully designed to capture the full breadth of programme learning outcomes, ensuring that students not only acquire technical competencies but also develop professional skills, including communication, teamwork, critical analysis, and problem-solving. By simulating workplace scenarios and aligning assessments with industry expectations, the strategy enhances employability and prepares graduates to operate effectively within complex organisational environments.

Assessment strategies are informed by current understanding of formative and summative evaluation in professional education contexts. Regular formative assessments through Blackboard's testing facilities provide immediate feedback, supporting research-backed spaced repetition and active recall techniques. Coursework design incorporates evidence from competency-based education research, ensuring students develop both technical skills and critical thinking abilities essential for cybersecurity professionals.

The programme adopts a programmatic assessment approach, where assessment activities are strategically sequenced and integrated across modules to provide multiple, complementary opportunities for students to demonstrate knowledge, skills, and professional attributes. This approach ensures inclusivity, supports enquiry-based learning, and encourages enterprising and reflective practice, equipping students to meet the evolving demands of the cyber security profession.

Student support: Pastoral Care:

At UWE, a wide range of services are available to provide pastoral care through its professional services, who offer comprehensive, full-time student support on a drop-in basis or by appointment. All students on the same route are allocated to consistent staff, who are trained to provide advice on commonly concerning matters, including regulatory issues. When necessary, the staff will direct the student to seek advice from other professional services.

Student Support and Guidance:

At UWE, student support is provided by academic staff, usually module leaders, for all issues relating to the content and delivery of the module. UWE student advice services offer timely, accurate, and confidential advice on all aspects of the provision, including fees, assessment arrangements, late work and extenuating circumstances procedures, timetabling, and progression counselling, as well as how to access the support provided by UWE.

Additional support and guidance are provided by Programme Leaders, who are responsible for ensuring the collection of and response to student feedback using student representatives through governance structures.

Further support is provided through the administration team, the admissions office, the Students' Union, the central University career service, and UWE’s counselling provision.

Students seeking employment opportunities during their studies have access to UWE’s career service and are encouraged to develop valuable skills by volunteering. There is support available for international students, including specific activities to assist international students in adapting to life in the UK, such as an additional induction week and specific literature to assist with their studies.

All students undergo a formal induction process to familiarise them with university life

and provide them with the means to access the support they may require during their studies at UWE. A student handbook documents this for students. A range of central services are offered to students, including for issues such as: money and finance advice; UWE's counselling provision; careers information; information technology services; student accommodation services; sports facilities; student union services; and the Chaplaincy.

Support for students with disabilities is offered centrally through UWE's disability service. The staff coordinate academic support for disabled students, including communicating individual students' support requirements to teaching and support staff and advising on reasonable adjustments to teaching and assessment. The staff also coordinate staff development on disability issues and provides information and advice to academic and support staff and students. Together, these services act as a holistic support system for disabled students and applicants to UWE, as well as supporting the academic and administrative staff who work with disabled students.

The career team provides various services and programmes to assist students in analysing their career interests, aptitudes, values, and goals. It also helps students with career planning and preparation for job interviews, in addition to providing job placement services for graduating students through networks with industry and potential employers. Its services include: career counselling; career talks and workshops; resume writing and grooming seminars; career-related fairs; and company visits.

An orientation programme is organised for all students before the start of the programme. It introduces students to the support available within the School and University through a range of speakers. An IT services orientation will introduce students to the email, VLE, and student portal.

International students will receive an induction from the international students service.

Part B: Programme Structure

Year 1

Full time students must take 180 credits from the modules in Year 1.
Part time students must take 60 credits from the modules in Year 1 and start the 60 credit Cyber Security Research Paper module which is continued and completed during year 2.

Year 1 Compulsory Modules (Part Time) (Year 1 and Year 2)

Part time students start the 60 credit Cyber Security Research Paper module in year 1 and complete in Year 2.

Module Code	Module Title	Credit
UFCE4B-60-M	Cyber Security Research Paper 2026-27	60

Year 1 Compulsory Modules (Full Time)

Full time students must take 180 credits from the modules in Compulsory Modules (Full Time).

Module Code	Module Title	Credit
UFCFVN-30-M	Computer and Network Security 2026-27	30
UFCF7P-15-M	Critical Systems Security 2026-27	15
UFCFFY-15-M	Cyber Security Analytics 2026-27	15
UFCFXN-15-M	Cyber Security Futures Emerging Trends and Challenges 2026-27	15
UFCE4B-60-M	Cyber Security Research Paper 2026-27	60
UFCE3Y-15-M	Digital Forensics for Cyber Security 2026-27	15
UFCFWN-15-M	Information Risk Management 2026-27	15
UFCF8P-15-M	IoT Systems Security 2026-27	15

Year 1 Compulsory Modules (Part Time)
Part time students must take 60 credits from the modules in Compulsory Modules (Part Time).

Module Code	Module Title	Credit
UFCFVN-30-M	Computer and Network Security 2026-27	30
UFCFFY-15-M	Cyber Security Analytics 2026-27	15
UFCFXN-15-M	Cyber Security Futures Emerging Trends and Challenges 2026-27	15

Year 2
Part time students must take 60 credits from the modules in Year 2 and complete the 60 credit Cyber Security Research Paper module which was started in Year 1.

Year 2 Compulsory Modules (Part Time)
Part time students must take 60 credits from the modules in Compulsory Modules (Part Time).

Module Code	Module Title	Credit
UFCF7P-15-M	Critical Systems Security 2027-28	15
UFCE3Y-15-M	Digital Forensics for Cyber Security 2027-28	15
UFCFWN-15-M	Information Risk Management 2027-28	15
UFCF8P-15-M	IoT Systems Security 2027-28	15

Part C: Higher Education Achievement Record (HEAR) Synopsis

On successful completion of this programme, graduates will have the appropriate knowledge, skills, and understanding to work at a senior technical level in the security domain of complex computer systems as well as roles in Information Security Consultant, Security Auditor etc. They will have a detailed understanding of computer and networks security and the context in which complex computer systems operate, including relevant legislation and standards. They will have specialised

knowledge of the technologies associated with complex secure systems (including industrial control systems and the Internet of Things), and the verification and testing of such systems.

Part D: External Reference Points and Benchmarks

In designing this programme, the following external reference points and benchmarks have been used:

QAA UK Quality Code for HE

NCSC – National Cyber Security Centre guidelines/requirements.

National qualification framework

Subject benchmark statement - Masters in Computing

QAA Master's degree characteristics

University strategies and policies

Industry consultation and external academic advice

The design of this programme and its associated module specifications aims to address skills shortages within the cyber security industry in the UK and, in particular, the South West and surrounding areas corridor. This shortage has been identified as a significant barrier to growth within industry reports ((ISC)2, NCSC), PSRB educational advisor / external academics, and range of industry professionals and collaborators.

This will align to UWE's strategy vision in encouraging and attracting more postgraduate students into education as another route for employment and skills development. UWE currently provides an undergraduate degree in this field. Feedback from students on this programme indicates that they would like the opportunity to further develop their skills in cyber security, either on a full-time or

part-time basis.

The programme structure and design are informed by QAA and National Cyber Security Centre (NCSC) recommendations incorporating a range of learning, teaching and assessment methods to prepare students for immediate entry into further study or employment. Aims and learning outcomes of the programme and modules have been explicitly designed to align with Master's level study as defined within the FHEQ / SEEC descriptors and the QAA qualification characteristics for Master's degrees, matching vocabulary where possible to make these links particularly clear.

Part E: Regulations

Approved to University Regulations and Procedures.