Programme Specification

Cyber Security and Digital Forensics {Foundation} [GCET]

Version: 2027-28, v1.0, 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 2

Part B: Programme Structure 7

Part C: Higher Education Achievement Record (HEAR) Synopsis 9

Part D: External Reference Points and Benchmarks 9

Part E: Regulations 10

Section 1: Key Programme Details

Part A: Programme Information

Programme title: Cyber Security and Digital Forensics {Foundation} [GCET]

Highest award: DipHE Cyber Security and Digital Forensics

Interim award: CertHE Cyber Security and Digital Forensics

Awarding institution: UWE Bristol

Affiliated institutions: GCET

Teaching institutions: GCET

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: Not applicable

Modes of delivery: Full-time

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

For implementation from: 01 September 2026

Programme code: G4ZC13

Section 2: Programme Overview, Aims and Learning Outcomes

Part A: Programme Overview, Aims and Learning Outcomes

Overview: The general aims of the programme are:

To prepare students for careers in computer security and computer crime-investigation (e.g. ‘forensic technician’).

To develop problem-solving, communication and other transferable skills applicable to a variety of careers.

To prepare students for study for higher degrees in related subjects.

Features of the programme: The foundation year acts as a vital stepping stone into the first year of the degree, designed to support students from diverse educational backgrounds in developing the broad academic and professional fundamentals required for higher-level study. Rather than focusing narrowly on subject-specific content, it provides a wide-ranging introduction to essential skills and concepts—including computational thinking, problem solving, academic literacy, project management, and effective communication. This generalist approach ensures that all learners, regardless of prior experience, build confidence in the core principles that underpin university-level learning. Alongside these transferable skills, students are introduced to best practices relevant to their subject area, laying the groundwork for deeper, discipline-specific engagement in subsequent years.

Educational Aims: The specific aims of the programme are:

To develop knowledge of computer hardware and software systems

To provide an understanding of applicable law, court procedure and the role of the expert witness

To introduce a variety of approaches to both the analysis of the security requirements of computer systems and the investigation of computer crime.

Programme Learning Outcomes:

On successful completion of this programme graduates will achieve the following learning outcomes.

Programme Learning Outcomes

PO1. Demonstrate an understanding of how computer systems and networks securely operate in the presences of threats.

PO2. Demonstrate understanding of the tools, and apply techniques for investigating computer crime and develop competence as a forensic computing practitioner.

PO3. Apply coherent knowledge and demonstrate understanding of legislation policies and regulations governing fields of cyber security and digital forensics.

PO4. Analyse security mechanisms and forensics frameworks for access control, encryption, digital signatures, and evidence preservation in digital case analysis.

PO5. Demonstrate understanding of security management policies and procedures by defining and modelling trust and security concepts, while ensuring secure access to services and diverse devices.

PO6. Demonstrate competency to use a variety of professional and academic literature sources to support independent research and enquiry.

PO7. Develop solutions to complex IT problems, involving uncertainty, that satisfy a range of stakeholder requirements.

Assessment strategy: Assessment strategies for this programme focus on ensuring a strong technical knowledge, use of appropriate tools, ability to devise and deploy security measures and an understanding of adversarial behaviours.

The programme implements a comprehensive assessment strategy that aligns with learning outcomes and professional requirements:

Diverse Assessment Methods:

Technical implementations and practical demonstrations

Written reports and documentation

Project presentations and demonstrations
Individual and group assignments
Research-based assessments

Professional Practice Assessment:

Evaluation of technical competencies
Assessment of professional skills and communication
Project management capabilities
Ethical consideration and responsible practice

Progressive Development:

Regular formative feedback throughout modules
Balanced distribution of assessments across the academic year
Integration of theoretical knowledge with practical applications
Focus on both individual and collaborative achievements

Industry Alignment:

Assessment tasks reflecting real-world scenarios
Emphasis on production-ready solutions
Evaluation of professional documentation and communication
Integration of current industry practices and standards

Quality Assurance:

Clear assessment criteria and learning outcomes
Regular review and updating of assessment methods
External examiner oversight

Alignment with university assessment regulations

This assessment strategy ensures graduates demonstrate both technical proficiency and professional capabilities required for successful careers in this field.

Student support: Pastoral Care:

Global College of Engineering and Technology (GCET) offers a wide range of services to provide pastoral care through professional services who provide comprehensive, full-time student support service. The professional services are trained to provide advice on matters commonly of concern, including regulatory and other matters.

Student Support and Guidance:

At GCET, student support is provided by academic staff, for all issues relating to the content and delivery of the module, and academic progress. Additional support and guidance is provided by Programme Leaders who are also responsible for gathering and acting upon student feedback and escalating issues through the appropriate governance structures.

Further support is provided through the administration team, the admissions office, career service and GCET's counselling provision. GCET also extensively supports students for placements services, in preparation for, as well as throughout, their study year abroad in UWE and acts both as an intermediary with UWE's other partner institutions and as a recruitment service for employers.

All students have a formal induction process to socialise them to their life in higher education and to provide them with the means to access the support that they may require during their study in GCET. Signposting to appropriate resources is provided.

Support to students with disability is offered centrally through professional support

services, who coordinate academic support for disabled students, including communication of student support requirements to teaching and support staff and advice and recommendations on reasonable adjustments to teaching and assessment. These act as a central service for disabled students and applicants to GCET and also support the academic and administrative staff members 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 assists students in career planning and preparation for job interviews, in addition to providing job placement services for graduating students through our network with industry and potential employers. It's services include career counselling, career talks and workshops, resume writing and grooming seminars, career-related fairs and company trips.

An orientation programme is organised for all students prior to the start of the programme and each year. It introduces students to the support available within GCET and UWE, via a range of events. There are additional events for international students.

Part B: Programme Structure

Year 1

Full time students must take 120 credits from the modules in Year 1.

Year 1 Compulsory Modules (Full Time)

Full time students must take 120 credits from the modules in Compulsory Modules (Full Time).

Module Code	Module Title	Credit
UFCEUF-30-0	Introduction to Speciality 2027-28	30
UFCEUP-30-0	Computational Thinking 2027-28	30

UFCEUS-30-0	Foundation Project 2027-28	30
UFCEV3-30-0	Professional and Communication Skills 2027-28	30

Year 2
Full time students must take 120 credits from the modules in Year 2.

Year 2 Compulsory Modules (Full Time)
Full time students must take 120 credits from the modules in Compulsory Modules (Full Time).

Module Code	Module Title	Credit
UFCF93-30-1	Computer and Network Systems 2028-29	30
UFCFP4-30-1	Computer Crime and Digital Evidence 2028-29	30
UFCFTK-30-1	Introduction to Databases 2028-29	30
UFCFGL-30-1	Programming for Cyber Security 2028-29	30

Year 3
Full time students must take 120 credits from the modules in Year 3.

Year 3 Compulsory Modules (Full Time)
Full time students must take 120 credits from the modules in Compulsory Modules (Full Time).

Module Code	Module Title	Credit
UFCEX5-30-2	Operating Systems and Software Security 2029-30	30
UFCE8B-30-2	Data Science for Cyber Security 2029-30	30
UFCFLC-30-2	Secure Computer Networks 2029-30	30
UFCFJ6-30-2	Security and Forensic Tools 2029-30	30

Part C: Higher Education Achievement Record (HEAR) Synopsis

Graduates would be expected to have an excellent understanding of the internal operation of computers and operating and file systems. They would be able to use appropriate tools to investigate computer-based activities, deploy tools and techniques to prevent security breaches and investigate the mis-use of computer systems and other devices. As much of this work is carried out either directly in support of legal processes an understanding of appropriate legal systems and law would be expected.

Part D: External Reference Points and Benchmarks

This programme is consistent with the UWE 2030 strategy in that its focus on the practice of computer security and forensics aligns with our aim of producing practice-oriented graduates.

The partnership with Taylors helps to ensure that the programme has an inclusive and global reach. The programme adopts the general approach of the school of Computing and Creative Technologies in including input from industry in terms both of visiting speakers and placement and work experience opportunities.

The QAA Computing and Law benchmark statements:

The QAA Subject Benchmark Statements for Computing (2022) and for Law (2023) are applicable to this programme.

The programme clearly falls into the cognate area described by the Computing benchmark. Due to the nature of Digital Forensic practice, much of the computing material is of a technical, low-level nature, with relatively little computing theory. Thus, in terms of the benchmark's high-level characterisation of Computing, the emphasis of the programme is on software, communication and interaction and practice, developed within the context of the specialised requirements of the programme. From the body of knowledge the following are considered essential to a study of Digital Forensics: Data Mining (in the context of forensic investigations); Computer Based Systems; Computer Networks; Data Structures and Algorithms, with emphasis on data structures; Distributed Computer Systems; Operating Systems; Programming Fundamentals; Security and Privacy; Web-based

Computing.

The Computing Benchmark Statement also contains (section 4) statements of the standards expected of graduates at both modal and threshold levels. The team is of the view that graduates of the proposed programme will be able to meet the required standards.

The Law benchmark has been considered during the design process at the 'Law as Subsidiary' level of performance, which focuses on the development of legal skills related to some specific area (in this case Digital Forensics). Though the Statement is targeted at programmes with at least 180 credits of legal subjects, its expectations also apply to programmes such as Digital Forensics, where the legal aspects make up a relatively small, but very important component. No attempt has been made to include all aspects of law or to provide the foundation for a legal career as such – instead the most important points of law and court procedure are covered. The aim of the design team has been to provide sufficient legal knowledge to be aware of the rules and legal system pertaining to Digital Forensics: as suggested in the Benchmark, the relevant law is treated mainly as data from which legal conclusions or opinions can be derived. It is expected that student will be able to assimilate legal information from a variety of sources and apply the knowledge acquired to computer crime investigation and security analysis.

Part E: Regulations

Approved to University Regulations and Procedures.

It is the Award Board's responsibility to determine whether the student's attainment at FHEQ Level 3 is sufficient to progress to Level 4.