Programme Specification

Computer Security and Forensics {Foundation} [GCET]

Version: 2023-24, v2.0, 24 Jan 2024

Contents

Section 1: Key Programme Details

Part A: Programme Information

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

Highest award: DipHE Computer Security and Forensics

Interim award: CertHE Computer Security and Forensics

Awarding institution: UWE Bristol

Affiliated institutions: Global College of Engineering and Technology (GCET)

Teaching institutions: Global College of Engineering and Technology (GCET)

Study abroad: Yes

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 October 2023

Programme code: G4HK00

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: Professional Practice and Lab Facilities:

Students can access a suite of newly purchased PCs (I7 and I5), modern software, free printing facilities and an IT help desk/line. The General IT lab is open from 8am till 9pm.

Besides the College’s plan of extending its IT facilities as the number of students grows, it also has a policy of upgrading 25% of its IT facilities every year.

Technology Enhanced Learning:

Staff members in the department are keen adopters of technology to support and enhance student learning. This includes:

Computer based e-assessment implemented in a number of modules, so that students can take regular short tests with automated computer generated feedback.

Recordings of some lectures (audio and video) which are made available after classes via the university’s Virtual Learning Environment.

Mathematics Support:

The Math Support Centre provides drop-in one-to-one tuition each day and a web-

site that provides a portal to a variety of on-line resources in mathematics and statistics.

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.

To prepare students for progression to bachelors level study and/or research into computer (cyber) security and (digital) forensics, or related disciplines.

Programme Learning Outcomes:

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

Programme Learning Outcomes

PO1. Apply knowledge, concepts and techniques of cyber security and digital forensics to offer feasible solutions to computer security and forensic problems.

PO2. Be able to use technical knowledge and skills to contribute to and deliver solutions through evidence-based enquiry

PO3. Be able to recognise security threats and their implications, plan actions and design systems to manage them.

PO4. Select and use appropriate techniques and tools to assess a computer crime scene and formulate a strategy for securing the evidence, investigating it impartially, and produce a report(s).

PO5. Be able to identify, security issues with computer networks, information and data in order manage security and trust in modern computer systems.

PO6. Respond to, and act upon the ethical, legal and professional implications of situations which they may encounter during their professional lives.

PO7. Be equipped to understand and respond to the changing needs of industry and society with respect to computer security and forensics.

Assessment strategy: The assessment strategy has been designed to test the programme learning outcomes.

Student support: Academic Support:

Academic advice and support is the responsibility of the staff delivering the module in question. Staff are expected to be available outside normal timetabled hours, either by appointment or during published "surgery" hours, in order to offer advice and guidance on matters relating to the material being taught and on its assessment.

Pastoral Care The College offers pastoral care through two routes:

Academic Personal Tutors: All level 4 students are assigned a Personal Academic Tutor, who is an academic member of staff in their department. Students meet individually with their tutor at least twice a year and also participate in group sessions with the Personal Academic Tutor’s tutor group (max size 15) during years 1 and 2.

Student Advisers, a team of administrative staff who provide comprehensive, full-time student support service on a drop-in basis or by appointment. Advisers are trained to provide advice on matters commonly of concern, including regulatory and other matters; the Adviser will, when necessary, advise the student to seek advice to from other professional services including the university's Centre for Student Affairs or from members of academic staff.

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
UFCFQN-30-0	Computational Thinking and Practice 2023-24	30
UFCFPN-30-0	Information Practitioner Foundations 2023-24	30
UFCE4A-15-0	Introduction to Creative Technologies 2023-24	15
UFME49-15-0	Introduction to Digital Design 2023-24	15
UFCFTN-30-0	Web Foundations 2023-24	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 2024-25	30
UFCFP4-30-1	Computer Crime and Digital Evidence 2024-25	30
UFCFC3-30-1	Introduction to OO Systems Development 2024-25	30

UFCFB3-30-1	Web Programming 2024-25	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
UFCE8B-30-2	Data Science for Cyber Security 2025-26	30
UFCFW5-30-2	Mobile and Embedded Devices 2025-26	30
UFCFLC-30-2	Secure Computer Networks 2025-26	30
UFCFJ6-30-2	Security and Forensic Tools 2025-26	30

Part C: Higher Education Achievement Record (HEAR) Synopsis
Graduates in this field 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 2020 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 GCET helps to ensure that the programme has an inclusive and global reach. The programme adopts the general approach of the department of Computer Science 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 and for Law were published in 2007, and are applicable to this programme.

The programme clearly falls into the cognate area described by the Computing benchmark. Due to the nature of Forensic Computing 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 Forensic Computing: 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 5) 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 Forensic Computing). Though the Statement is targeted at programmes with at least 180 credits of legal subjects, its expectations also apply to programmes such as Forensic Computing, 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 Forensic Computing: 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.