Programme Specification

Section 1: Basic Data

Awarding institution/body	University of the West of England
Teaching institution	University of the West of England
Faculty responsible for programme	Computing, Engineering and Mathematical Sciences
Programme accredited by	N/A
Highest award title	BSc (Hons) Forensic Computing
Default award title	
Interim award title	BSc Forensic Computing Diploma of HE, Forensic Computing Certificate of HE, Forensic Computing
Modular Scheme title (if different)	
UCAS code (or other coding system if relevant)	
Relevant QAA subject benchmarking group(s)	Computing (primary) Law (secondary)
On-going/valid until* (*delete as appropriate/insert end date)	
Valid from (insert date if appropriate)	1st September 2005

Authorised by… **Date:…**

Version Code 1

For coding purposes, a numerical sequence (1, 2, 3 etc.) should be used for successive programme specifications where 2 replaces 1, and where there are no concurrent specifications. A sequential decimal numbering (1.1; 1.2, 2.1; 2.2 etc) should be used where there are different and concurrent programme specifications

Section 2: Educational Aims of the Programme

The general aims of the programme are:

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

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 investigation of computer crime and the analysis of the security requirements of computer systems

Section 3: Learning Outcomes of the Programme

The programme route provides opportunities for students to develop and demonstrate knowledge and understanding, intellectual skills, subject-specific skills and transferable skills, as shown below.

A. Knowledge and Understanding

Knowledge and Understanding of:	Teaching/Learning Methods and Strategies	Assessment
1. Computer systems and networks	During the first year, students are introduced to basic programming skills and gain practical knowledge in constructing simple software systems. They encounter the elementary components of computer systems. This knowledge is extended during the second year to give the knowledge necessary to understand different computer architectures and network topologies.	Assessment will be by a combination of examination and coursework. For many aspects of this programme the coursework will contain a significant practical element. Where appropriate other forms of assessment such as observation of a presentation or viva may be used. The nature of Forensic Computing implies a significant inter-disciplinary component. For example, the student might research into some aspect of the law as it applies to Forensic Computing or a relevant legal case. The student would then be required to evaluate the evidence and relevant law precedents, form an opinion and produce a written report. Alternatively, the student might be given a unique set of data representing a possible computer crime scene and, applying their computer and legal skills, investigate this, produce a report suitable for use by the legal profession and then defend their work during a viva. Communication skills form an important part of the programme. These would be assessed mock trial and final year viva.
2. Information, data and its representation and organisation in computer systems	Beginning in the first year with data modelling techniques and continuing into the second year with schemas, students learn how information can be represented as data within a computer.	
3. The English legal system and court procedure	Will conform to the QAA subject benchmarking for Law, treating the law component of the programme as 'subsidiary'. Students will be introduced to the principle features of the English legal system , its institutions and procedures. Criminal process and PACE will be highlighted. The role of judges, barristers, solicitors and court staff will be explained in the first year and witnessed during visits to appropriate proceedings. In the second year students will take part in a mock trial.	
4. Law pertaining to computer crime and digital evidence and its investigation	Throughout the programme students are exposed legal terminology and legal texts. A first-year module introduces computer crime legislation including Computer Misuse Act 1990, EU CyberCrime Convention 2003 and relevant international law. Categories of computer crime: offences against	

	confidentiality and integrity; computer-related; content-related. UK law pertaining to seizure and presentation as evidence is then covered, for example Police and Criminal Evidence Act, 1984, Regulation of Investigatory Powers Act 2000. Finally difficulties and emerging issues in interpreting these laws are discussed.	
5. Tools and techniques for investigating computer crime such as data mining and profiling	Securing and examining evidence will be introduced using the platform of industry-standard software such as EnCase and other generic investigative tools. These tools will be available for student use in investigating sample data. In the final year the project provides for the investigation of and reporting on a substantial set of data. Throughout there is an emphasis on preventing contamination of the evidence, ensuring continuity of evidence and the use of auditable procedures.	
6. Skills and responsibilities of a forensic computing practitioner and expert witness	Communication skills, both written and verbal, with a legal context are introduced during the second year. The students will gain experience of the requirements of the legal system in terms of admissibility of evidence, its presentation in a form suitable for legal use and its defence during legal hearings. In the final year project students will investigate a complex set of data, prepare a written report and then defend it in a viva situation.	
7. Computer security and computer crime prevention	Modes of attacking and defending computer systems will be covered with practical examples. Topics will include: (modes of attack) viruses, worms, trojans, hacking; (defence mechanisms) security protocols, cryptography, digital watermarking, hardware techniques.	

B. Intellectual Skills

Intellectual Skills	*Teaching/Learning Methods and Strategies*	*Assessment*
1. Critical Thinking 2. Analysis 3. Synthesis of different types of information 4. Evaluation 5. Problem Solving 6. Appreciate problem contexts 7. Balance conflicting objectives	At all levels students are required to bring together knowledge and skills acquired in different subsidiary disciplines and hence determine new ways of approaching problems. As the student progresses, the need to synthesise (3) ever-greater volumes of information and requirements into a coherent approach is developed and consequently so is their critical thinking (1). At level 1 Analysis (2), Evaluation (4) and Problem Solving (5) are developed on small-scale problems in various computing and law-based activities in a number of modules. At this level the focus is on understanding the problem and then solving it in simplified environments, often without the need to examine alternatives and to balance conflicting goals. At level 2 there is a move away from small-scale problems to the investigation of computer crime as part of the legal process and the analysis and implementation of security systems in a real-world context. With this comes the need to evaluate (4) appropriate approaches, understand the context of legal and ethical requirements (6) and to balance conflicting objectives (7). Level 3 sees the move to complex situations where it will be necessary to use all the intellectual skills acquired earlier in the programme to achieve an appropriate and fair representation of a representative computer crime scene.	The investigation of computer crime evidence requires demonstration of all of the intellectual skills. At level 1 the focus in programming coursework assessment, undertaken in a number of modules, is on the skills of Analysis (2), Evaluation (4) and Problem Solving (5). At levels 2 and 3 this branches out to include all the remaining skills. Many of the coursework assessments and exam papers include elements of programming work. Independent reading is used to enable students to focus on their own areas of interest and in the process assess skills 1-4 in the submitted reports, essays and exam answers. Design-work, even when not implemented in a programming language, requires demonstration of skills 1,2,5,6,7 and a number of coursework assessments and exam questions are devoted to such work. Finally, all of the examinations assess skills 1-4 whilst skills 5-7 are covered in many exams.

C. Subject, Professional and Practical Skills

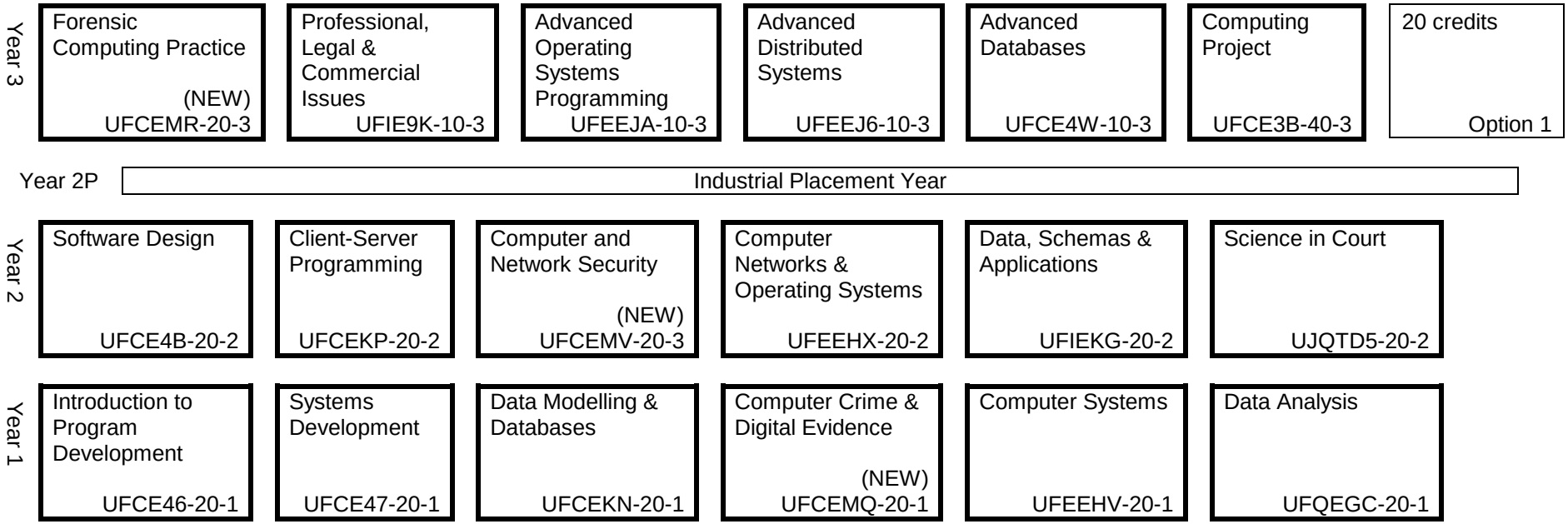
Subject/Professional/Practical Skills	***Teaching/Learning Methods and Strategies***	***Assessment***
Students will be able to: 1. Understand a variety of computer systems, configurations and networking topologies 2. Understand the professional and legal obligations of forensic computing investigations 3. Be able to communicate with legal personnel at an appropriate level 4. Be able to assess a computer crime scene and formulate a strategy for securing the evidence, investigating it impartially, and produce a report in appropriate language 5. Select and use appropriate forensic tools 6. Know the limits of their knowledge and how to extend those limits through self-managed learning 7. Analyse and implement computer security measures 8. Write programs that conform to designs 9. Employ a range of tools and notations to support the activities listed above: e.g. forensic computing tools, editors, compilers, HTML, CGI, Java etc.	Throughout the program, the skills listed are developed through a combination of theoretical discussion, practical laboratory based work, classroom based tutorial exercises and directed self-study. Most of the skills listed (1, 2, 3, 4, 5, 6, 8, 9) are introduced at level 1 and then drawn into sharper focus at levels 2 and 3. The general teaching/learning method is therefore to impart these practical/professional skills by a process of moving from an overview of what is required to a specific application of an individual skill at a higher level. Security-based skills (7) are introduced at level 2 and continued into level 3.	A combination of all or most of these skills will be required to successfully complete the final year project The possession of these skills is demonstrated both by the investigation of a potential computer crime scene and by examination. The practical nature of the skills to be acquired means that some are specifically addressed by particular modules (2, 3, 4, 6, 7). The more generic skills (1, 6, 9) are assessed across the programme. .

D. Transferable Skills and Other Attributes

Transferable Skills and Other Attributes	***Teaching/Learning Methods and Strategies***	***Assessment***
1. Communication skills**:** to communicate orally or in writing, including, for instance, the results of technical investigations, to peers and/or to "problem owners".	1. Skill one is developed through a variety of methods and strategies including the following: ♦ Students maintain laboratory log books ♦ Students participate in electronic conferences, workshops, and groupwork sessions. ♦ Students participate in discussion tutorials ♦ Students present research topic findings in tutorials ♦ Students participate in individual tutorials ♦ Students participate in mock trials, cross-examination and other verbal interrogation	These skills are demonstrated in a variety of contexts including • Examination • Poster presentation, individual and group projects • Practical assignments • Portfolio of exercises • Mock trial • Viva
2. Self-management skills: to manage one's own time; to meet deadlines; to work with others having gained insights into the problems of team-based systems development.	2. Skill two is developed through a variety of methods and strategies including the following: ♦ Students conduct self-managed practical work ♦ Students participate in practically-oriented tutorial laboratory sessions ♦ Students work through practical work-sheets in teams ♦ Students practice design and programming	
3. IT Skills in Context (to use software in the context of problem-solving investigations, and to interpret findings)	3. Skill three is developed widely throughout the programme.	
4. Problem formulation: To express problems in appropriate notations.	4. Skill four is developed through a variety of methods and strategies including the following: ♦ Students practice design and programming ♦ Students devise procedures for investigating digital evidence	
5. Progression to independent learning: To gain experience of, and to develop skills in, learning independently of structured class work. For example, to develop the ability to use on-line facilities to further self-study.	5. Skill five is developed through a variety of methods and strategies including the following: ♦ Students are encouraged to practice programming to extend their skills ♦ Students are encouraged to research relevant computing and law topics ♦ Students are encouraged to use online facilities to discover information	

6. Comprehension of professional literature: to read and to use literature sources appropriate to the discipline to support learning activities.	6. Skill six is developed through a variety of methods and strategies including the following: ♦ Students are encouraged to read legal case notes ♦ Students are encouraged to maintain their awareness of computing and security issues via both printed and online materials	
7. Working with Others**:** to be able to work as a member of a team; to be aware of the benefits and problems which teamwork can bring.	7. Skill seven is developed through a variety of methods and strategies including the following: ♦ Students carry out work in small, self-managed groups	

Section 4: Programme Structure



Option 1 taken from	
UFCE3K-20-3	Machine Learning
UFCE4P-10-3	Object-Oriented Databases
UFCE4Q-10-3	Parallel and Distributed Databases
UFCEMU-20-3	Cryptography and Coding Systems
UFIE8M-20-3	Information Systems Management
UFIE9S-20-3	Multimedia Systems: Context & Applications
UFIEMF-20-3	Data Mining Methodology

PLEASE NOTE: REFER TO THE FACULTY ON-LINE INFORMATION SYSTEM FOR UP-TO-DATE STRUCTURE INFORMATION

http://www.cems.uwe.ac.uk/exist/index.xql

Section 5: Entry Requirements

The university's minimum requirements for entry to a degree apply to this programme. In addition entrants are required to have evidence of achievement in Mathematics at GCSE Grade C or equivalent.

Section 6: Assessment Regulations

The Modular Assessment Regulations apply to this programme

Section 7: Student Learning: Distinctive Features and Support

Class Activities The mode of delivery of a module is determined by its Module Leader, and typically involves a combination of one or more lectures, tutorials, 'lectorials', laboratory classes, group activities and individual project work. Modules are often delivered by means of 'lectorials', classes for groups of 20-30 students with no distinction between lectures and tutorials, and this has proved to be an effective mechanism for modules at Level 1.
Where modules are common with other programmes, students will typically be taught together (which gives students the opportunity to appreciate the material from the viewpoint of different engineering disciplines). However, a specialist flavour may be given to a common module through the provision of discipline specific practical, laboratory or tutorial material supporting a core of common lectures.

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..

Virtual Learning Environment
The faculty is in the process of developing its presence on UWEOnline, the university's virtual learning environment. In 2003-04, a total of over 40 of the faculty's modules are using UWEOnline to assist in delivery, and this academic year the number has increased to 115. The faculty's goal, as expressed in it's Teaching and Learning strategy document, is to have a presence on UWEOnline for all modules once technological constraints permit.

Pastoral Care The faculty's offers pastoral care through its Student Advisers, a team of staff who provide comprehensive, full-time student support service on a drop-in basis or by appointment. All students on the same route are allocated to the same Adviser, who is 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.

Progression to Independent Study
Many modules require students to carry out independent study, such as research for projects and assignments, and a full range of facilities are available at all sites to help students with these. The philosophy is accordingly to offer students both guided support and opportunities for independent study. Guided support, mainly in the form of timetabled sessions, takes the form of lectures, tutorials, seminars and practical laboratory sessions. Students are expected to attend all sessions on their timetable, and this is especially important because of the high content of practical work in the programme.

The progression to independent study will also be assisted by the nature of the support offered in individual modules. Typically, module leaders will provide a plan for the module indicating the activities to be carried out and the forms of learning to be undertaken during the delivery of the

module, with a view to encouraging students to plan ahead and to take responsibility for managing their time and resources.

Computing Facilities The Faculty offers a specialised computing facility along side the general University provisions. There are nine general PC computing laboratories of 20 plus seats all running Windows2000, along with four Unix based laboratory and 10 specialist computing labs. The specialist laboratories are equipped with the specific software for CEMS students; including Software Design Tools development environment, CAD, finite element analysis, mathematics and statistics packages to support the taught program. The specialist Computing laboratories are designed to target the discipline taught in that area. Amongst these, is the Computer Systems Architecture and Linux laboratory. The Unix labs offer the latest web development and programming tools.

One of the most popular areas within the Faculty is the Open Access laboratory. This area is never time-tabled and gives students the opportunity to access machines at all times during opening hours. This is a mixed environment consisting of PCs and Unix workstations.

Due to the extensive computing facility provided within the Faculty, and the specialist nature of this facility, the need for user support is necessary. The Faculty provides a user support Helpdesk. The Helpdesk provides first line support to the user base, uniquely supported by both permanent staff and students in their second or final year of study (employed on a part time basis) until 20.00hrs every day. These general purpose and specialist laboratories are available to students up until midnight, seven days per week

Section 8 Reference Points/Benchmarks

The QAA Subject Benchmark Statements for Computing and for Law were published in 2000, and are applicable to this proposal.

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: *Artificial Intelligence*, specifically in the context of data mining; *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.