Title of Module: Cyber Security: Law and Ethics

Code: COMP11086	**SCQF Level: 11** **(Scottish Credit and Qualifications Framework)**	**Credit Points: 10**	**ECTS: 5** **(European Credit Transfer Scheme)**
School:	School of Computing, Engineering and Physical Sciences		
Module Co-ordinator:	Malcolm Bronte-Stewart (now Junkang Feng)		

Summary of Module

This module provides students with an understanding of the ethical issues and codes of practice together with the moral and professional responsibilities of the cyber security practitioner. An overview of ethical and legislative issues relevant to cyber security are discussed together with systems thinking and critical evaluation. It considers and reflects upon the implications and impacts of aspects of cybersecurity.

This module will work to develop a number of the key **'I am UWS' Graduate Attributes** to make those who complete this module:

Universal

- Critical Thinker
- Ethically-minded
- Research-minded

Work Ready

- Problem-Solver
- Effective Communicator
- Ambitious

Successful

- Autonomous
- Resilient
- Driven

Module Delivery Method		
Face-To-Face	**Blended**	**Fully Online**
	✓	
Blended A mode of delivery of a module or a programme that involves online and face-to-face delivery of learning, teaching and assessment activities, student support and feedback. A programme may be considered "blended" if it includes a combination of face-to-face, online and blended modules. If an online programme has any compulsory face-to-face and campus elements it must be described as blended with clearly articulated delivery information to manage student expectations		

Learning Outcomes: (maximum of 5 statements)
On successful completion of this module the student will be able to: L1. Demonstrate a critical understanding of the theories, concepts and principles of legislative and regulatory frameworks, and ethics related to cyber security; L2. Apply knowledge, skills and understanding to undertake professional activities legally and ethically. L3. Critically evaluate the laws and ethics relating to cyber crime.

Employability Skills and Personal Development Planning (PDP) Skills	
SCQF Headings	During completion of this module, there will be an opportunity to achieve core skills in:
Knowledge and Understanding (K and U)	SCQF Level 11. Students will learn the theories, concepts and principles of legislative and regulatory frameworks, and ethics related to cyber security
Practice: Applied Knowledge and Understanding	SCQF Level 11. Students will gain in-depth, comprehensive understanding, knowledge and skills undertake professional activities legally and ethically.
Generic Cognitive skills	SCQF Level 11. To complete their written reports and laboratory tasks, students will first build skills to integrate information and apply knowledge from various sources including technology advances informed by research and industry.
Communication, ICT and Numeracy Skills	SCQF Level 11. Working in groups, students will develop communication skills as well as the ability to write technical reports and documentation.
Autonomy, Accountability and Working with others	SCQF Level 11.

	Exercise a substantial ability to work autonomously, demonstrating critical inquiry in producing quality work underpinned by rigorous investigation. Learn effectively for the purpose of continuing personal development planning through interacting with others in academic and professional bodies and organisations relevant to m-business. Demonstrate an ability to manage and work autonomously with a range of self-directed m-business related learning resources.

Learning and Teaching

The module will be delivered by means of lectures and supervised hands-on lab work. Lectures will cover the theoretical background and practical applicability in real life problems. Concepts will be introduced by posing a practical problem and working out the needed theoretical knowledge to solve them. The delivery will encourage student participation to ensure an active learning experience. Group discussions will be held to promote critical thinking and boost informed decisions on the suitability of different state-of-the-art methods. Lab exercises will help student develop their knowledge in incremental fashion using a learning-by-doing approach. This will support the development of knowledge and understanding of the topics.

Learning Activities During completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	**Student Learning Hours** (Normally totalling 200 hours): (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture/Core Content Delivery	10
Tutorial/Synchronous Support Activity	5
Tutorial/Synchronous Support Activity	9
Independent Study	76
	100 Hours Total

****Indicative Resources: (eg. Core text, journals, internet access)**

The following materials form essential underpinning for the module content and ultimately for the learning outcomes:

Manjikian, M. (2017) Cybersecurity Ethics: An Introduction. Routledge.

Etzioni, A and Rice, C.J. (2015) Privacy in a Cyber Age: Policy and Practice. Palgrave Macmillan

Alfreda Dudley, A., Braman, J. and Vincenti, G. (2012) Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices. IGI Global.

Kosseff, Jeff, (2017) Cybersecurity Law, Wiley

Schaub, Gary, (2018) Understanding cybersecurity: emerging governance and strategy, Rowman and Littlefield International Ltd.

(**N.B. Although reading lists should include current publications, students are advised (particularly for material marked with an asterisk*) to wait until the start of session for confirmation of the most up-to-date material)

Attendance Requirements

In line with the Academic Engagement and Attendance Procedure, Students are defined as academically engaged if they are regularly engaged with timetabled teaching sessions, course-related learning resources including those in the Library and on Moodle, and complete assessments and submit these on time. Please refer to the Academic Engagement and Attendance Procedure at the following link: Academic engagement and attendance procedure

Assessment: (also refer to Assessment Outcomes Grids below)

Coursework (100%)

(N.B. (i) **Assessment Outcomes Grids** for the module (one for each component) can be found below which clearly demonstrate how the learning outcomes of the module will be assessed.
(ii) An **indicative schedule** listing approximate times within the academic calendar when assessment is likely to feature will be provided within the Student Handbook.)

Assessment Outcome Grids (Footnote A.)

Component 1					
Assessment Type (Footnote B.)	**Learning Outcome (1)**	**Learning Outcome (2)**	**Learning Outcome (3)**	**Weighting (%) of Assessment Element**	**Timetabled Contact Hours**
Report of practical/ field/ clinical work	✓	✓	✓	80	0
Presentation	✓	✓	✓	20	1
Combined Total For All Components				100%	1 hours