1. **Title of the module**

COMP8410 (CO841) - Cyber Law

1. **School or partner institution which will be responsible for management of the module**

School of Computing

1. **The level of the module (e.g. Level 4, Level 5, Level 6 or Level 7)**

Level 7

1. **The number of credits and the ECTS value which the module represents**

15 credits (7.5 ECTS)

1. **Which term(s) the module is to be taught in (or other teaching pattern)**

Autumn or Spring

1. **Prerequisite and co-requisite modules**

None

1. **The programmes of study to which the module contributes**

Portfolio of taught postgraduate programmes in Computing
(compulsory for MSc Cyber Security)

1. **The intended subject specific learning outcomes.
On successfully completing the module, students will be able to:**

8.1 Demonstrate an advanced grounding in concepts, ethics, principles and rules of cyber security, data protection, consent and privacy in a legal context

8.2 Demonstrate a systematic understanding of the development of EU, UK and US laws related to cyber security, cybercrime, digital investigation, privacy and data protection, including domestic legislation and emphasising cross-boundary issues and international efforts.

8.3 Critically analyse emerging legal issues in cyber security, cybercrime, privacy and data protection, for example: big data, social media, data anonymization, data access controls, state and commercial surveillance.

8.4 Demonstrate a critical awareness of, and the ability to evaluate, legal and regulatory actions taken to ensure cyber security, privacy and data protection, including legal governance and compliance requirements.

8.5 Demonstrate a critical understanding of the public and private tensions involved in cyber security, cybercrime, privacy and data protection.

1. **The intended generic learning outcomes.
On successfully completing the module, students will be able to:**

9.1 Present relevant knowledge and understanding in the form of an original and reasoned argument.

9.2 Identify, analyse and critically evaluate complex problems.

9.3 Carry out independent research from a variety of sources informing an original, sustained and detailed argument.

9.4 Summarise detailed conceptual material, recognising, critically evaluating and synthesising different positions that arise in the literature surveyed.

1. **A synopsis of the curriculum**

The module will explore existing and emerging legal issues in cyber security, cybercrime, privacy and data protection, including the domestic and cross-boundary legal regulatory frames and their associated ethical dimensions. Topics covered include cybercrime, privacy and data protection, Internet and cyber surveillance, cross-border information flows, and legal structures. Students will be challenged to critically examine the ethics and management of cyber data. It will require students to assess emerging legal, regulatory, privacy and data protection issues raised by access to personal information.

1. **Reading list (Indicative list, current at time of publication. Reading lists will be published annually)**

P. Carey, *Data Protection: a practical guide to UK and EU Law* (Oxford University Press, 2009).

M. Johnson, *Cyber Crime, Security and Digital Intelligence* (ePub Ashgate, 2013).

L. Katz, (2013) *‘Symposium on Cybercrime’*. Journal of Criminal Law and Criminology, 103 (3).

C. Kunar, *International Data Privacy Law* (Oxford University Press, 2013).

D. Solove, P. Schwartz, *Privacy, Information, and Technology, 3rd edition* (Aspen Publishing Co., 2012).

H. Tse, *Cyber Security Law and Guidance* (Bloomsbury Press, 2018)

1. **Learning and teaching methods**

Contact hours: 20

Private study hours: 130

Total study hours: 150

1. **Assessment methods.**

13.1 Main assessment methods

Two written assessments. Assessment 1 maximum 1500 words (40%); Assessment 2 maximum 2500 (60%).

13.2 Reassessment methods

Like-for-like

1. ***Map of module learning outcomes (sections 8 & 9) to learning and teaching methods (section 12) and methods of assessment (section 13)***

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Module learning outcome** | 8.1 | 8.2 | 8.3 | 8.4 | 8.5 | 9.1 | 9.2 | 9.3 | 9.4 |
| **Learning / teaching method** |  |  |  |  |  |  |  |  |  |
| Lectures and seminars | x | x |  | x |  | x | x | x |  |
| Private study | x | x | x |  | x |  |  | x | x |
| **Assessment method** |  |  |  |  |  |  |  |  |  |
| Written assessments | x | x | x | x | x | x | x | x | x |

1. **Inclusive module design**

The School recognises and has embedded the expectations of current equality legislation, by ensuring that the module is as accessible as possible by design. Additional alternative arrangements for students with Inclusive Learning Plans (ILPs)/declared disabilities will be made on an individual basis, in consultation with the relevant policies and support services.

The inclusive practices in the guidance (see Annex B Appendix A) have been considered in order to support all students in the following areas:

a) Accessible resources and curriculum

b) Learning, teaching and assessment methods

1. **Campus(es) or centre(s) where module will be delivered:**

Canterbury

1. **Internationalisation**

Internationalisation is fully supported throughout the delivery of the curriculum with comparisons made with other jurisdictions weekly and consideration given to the way in which other jurisdiction develop their approach to cyber security. Students are actively encouraged to make use of international resources in their research in order to critically engage with the questions posed and compare different approaches

**DIVISIONAL SUPPORT OFFICE USE ONLY**

**Revision record – all revisions must be recorded in the grid and full details of the change retained in the appropriate committee records.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date approved | Major/minor revision | Start date of the delivery of revised version | Section revised | Impacts PLOs(Q6 & 7 cover sheet) |
| 09/05/2018 | Major | September 2018 | 1, 5, 7, 8, 9, 10, 11, 12, 13, 14 |  |
|  |  | September 2020 | 13 |  |