Module Title **Computer Ethics and Law** **Keywords** Ethics, law, professionalism, privacy, sharing, hacking, human errors, cyber-warfare and defence	Reference CM3100 SCQF Level SCQF 9 SCQF Points 15 ECTS Points 7.5 Created March 2007 Approved July 2016 Amended April 2016 Version No. 1

This Version is No Longer Current

The latest version of this module is available here

Prerequisites for Module

CM2102 Real World Project & Professional Skills, or equivalent.

Corequisite Modules

None.

Precluded Modules

None.

Aims of Module

To provide students with the ability to independently and as a team member identify, analyse, discuss and report key issues of ethics and law that relate to computer security for both individuals and society. Students will also be provided with an opportunity to explore and understand the importance of the Interpreting laws and approaches to ethical analysis; case studies. Human in the loop; human errors and security vulnerabilities and how to counter them. Analytical skills and systematic analysis; debating, reporting, writing and oral skills. Cyber terrorism; cyber defence; professional roles.

Standards and Best Practice Guides: ISO 27001, ISO 27014, ISO 27036.

Indicative Student Workload

Contact Hours	Full Time
Labs	18
Lectures	18
Directed Study	
Directed Reading	36
Private Study	

roles users play in cyber security. This includes positive and negative aspects, human error versus premeditated actions and behaviours.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1. Identify important ethical and legal issues that impact on professional behaviour linked to computer security
2. Research and analyse material and real-world situations that relate to ethical and legal issues linked to human aspects of security.
3. Systematically debate, discuss and report the outcomes of investigations.
4. Provide advice and recommendations about how to tackle ethical and legal issues linked to security.
5. Apply industry standards and guides of best practice to situations involving information security.

Indicative Module Content

Legal and ethical frameworks; codes of conduct and professional societies.
Modern security concerns and cyber issues; privacy, sharing;

Private Study	78

Mode of Delivery

This module is delivered through lectures, tutorials and assessed practical work with formative feedback.

Assessment Plan

	Learning Outcomes Assessed
Component 1	1,2,3,4,5

Component 1 - Coursework totalling 100% of the total module assessment.

Indicative Bibliography

1. MANJIKIAN, M. 2018. Cybersecurity Ethics: An Introduction. Taylor & Francis
2. TAVANI, H. T., 2013. Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing. 4th ed. Wiley.
3. FRIEDMAN, B., HENDRY, D. G. 2019. Value Sensitive Design: Shaping Technology with Moral Imagination. MIT Press

hacking.