

## **MRes Information Systems modules 2012-13**

### **Critical Reading**

To become an effective researcher requires the ability to rapidly assimilate and assess large amounts of information. One of the most effective means of achieving this is to read and critique academic and scientific materials that are related to a given area. The means by which these materials are accessed has changed dramatically over recent years, but the core skills of critical reading remain unchanged. This module will equip students with robust critical reading skills, which will provide a foundation for other research techniques. On completion of the module students will be able to synthesise a large body of work and manage literature using a range of tools.

### **Information, Network and Cyber Security**

This module focuses on the concepts of information security within the context of an organisation's IT and information systems. The fundamentals of network security are taught, from internal networks through to issues arising from Cloud computing. The module introduces the skills required for risk assessment and to design information security policies in line with standards, legal and ethical aspects of information security. The technical concepts of cryptography are introduced, and students will be taught to evaluate and use applications to secure information, networks, and manage personal identities.

### **Organisations, Complexity and Systems**

This module examines the nature of complexity within modern organisations and introduces concepts, methods and ways of thinking that can deal with such systems. In particular it will present different ways of looking at the organisation and will consider the characteristics of methodologies appropriate for modelling organisational problems. Students will practice developing qualitative models which will influence information systems designers and enterprise managers in their decision making. Using the Systems Thinking methodology, models of business processes and supporting IT infrastructure will be developed. This will enhance abilities in gathering and assessing a project's needs and requirements and involves constructing competing arguments in the context of information systems design and implementation.

### **Research and Entrepreneurship Skills**

This module aims to equip the student with skills to undertake research in their chosen field on a practical basis. A short supervised project will be undertaken to develop methodological design and implementation skills as relevant to a particular area. The module pays attention to the impact that research can have on the wider world. The fundamentals of intellectual property rights are explored, as are the entrepreneurship skills associated with exploiting research. Legal, ethical, societal and professional issues and business planning are tackled with reference to the steps associated with establishing a business in the technology sector.

### **Research Rigour and Investigation**

Sustained, successful research often arises from the diligent, rigorous and transparent pursuit of a hypothesis. Since new research often builds on the results and methods developed from previous work, it is important to be able to replicate and validate published results. The module develops a professional and ethical understanding of the quantitative and qualitative methods of scientific research, peer review and academic publishing. From undertaking the module, students will be able to critically assess and validate academic contributions to the state-of-the-art.

### **Security Techniques**

It is essential for a security professional to understand the technology available to them and harmonise an approach to technical systems and network security with enterprise requirements and policy. This module focuses on the fundamental technical security techniques and technologies available to security professionals, within the context of modern, pervasive communications and distributed networks and systems. Security technologies such as encryption, access control and methods of authentication are examined in detail with technical explanation of the fundamental computer science that underpin them. These are viewed alongside potential threats such as eavesdropping, network attacks and the vulnerabilities of data as it moves between systems. There is a technical focus on cryptography, its history and current modes of operation.