What did we cover?

- English Law (Civil versus Criminal & Tort)
  - Computer Misuse Act
  - Data Protection Act
  - Freedom of Information
  - Intellectual Property
  - Contract Law
  - The Internet – Defamation Act, Obscene Publications Act etc.
  - Employment Law
- Communication Skills
  - Presentations
  - CVs
  - Technical Writing
- Ethics & Professionalism
Learning Outcomes

• After the end of this module, you should be able to: Identify, demonstrate an understanding of and describe ethical, social, legal and professional issues in computing. (Exam/Coursework)

• Discuss these issues in a balanced and lucid way. (Coursework)

• Make good presentations of views in a formal report format. (Coursework)
The Exam

• Professional Computing was a new module for 2012/13
• One Past Paper is now available!

1. The Exam consists of four short questions
   1. Key topics
   2. Computer Misuse Act
   3. Data Protection Act
   4. Human Resources
   5. Privacy & Internet Issues
   6. Ethics

I don’t expect the exam to be hard but there are some things every IT professional really should know …
Computer Misuse Act (1990)

- Three Offences
  - Unauthorized access to a computer;
  - Unauthorized access to a computer to commit a serious crime; and
  - Unauthorized modification of the contents of a computer.

- A person is guilty of a crime if either they or the computer in question is in the UK at the time of the offence.
Unauthorized Access Offence

Section 1

- A person is guilty of an office if
  - He causes a computer to perform any function with intent to secure access to any program or data held in any computer;
  - The access he intends to secure is unauthorised; and
  - He knows at the time when he causes the computer to perform the function that this is the case

- Punishable by a fine up to £5000 or 6 months imprisonment
- (upgraded in 2006 to 1 year or a fine up to statutory maximum or both)

Key points:

Knowledge & intent
Attempt is sufficient
No requirement of damage done
Upgrade means it is now a “serious” crime and therefore extraditable
Intent to do serious crime

- Section 2 covers unauthorized computer access to commit a more serious crime.
  - E.g. a blackmailer might hack into email to gain evidence of an affair etc.
  - It is not necessary for the more serious crime to be carried out … as long as intent to do so can be shown.

- Punishment is up to five years imprisonment or an unlimited fine.
Unauthorized Modification

• A person is guilty of an offence if
  • he does any act which causes an unauthorized modification of the contents of any computer; and
  • At the time when he does the act he has the requisite intent and the requisite knowledge.

• Requisite intent covers:
  • To impair the operation of any computer;
  • To prevent or hinder access to any program or data held in any computer; or
  • To impair the operation of any such program or the reliability of any such data

• Maximum penalty is 5 years or unlimited fine.
  • Spreading a virus
  • Encrypting files and demanding a ransom for revealing the key
  • Redirection of browser home pages etc etc.
CMA Question

• Summarise the three sections of the Computer Misuse Act. A word for word repetition of the act is not required. However you should clearly distinguish the three offences described by the act and any differences between these offences.

• A student on your course notices that the Exams Officer keeps a copy of the password for the 2014/2015 exam database on a post it note attached to his computer and shares the password with you. You realise that looking at past papers with their model answers would really help your revision and so decide to log in as the Exams Officer and take a look.

• Comment on whether such an action would infringe the Computer Misuse Act. In addition comment on whether you or any other involved party might be liable to either legal or university sanction and justify your answer.
Exam cheat jailed for hacking into university computer system

Court hears University of Birmingham student Imran Uddin, 25, used a keyboard spying device to steal staff passwords and then upped five exam marks.
Data Protection Act

• First Principle
  • Personal data will be processed fairly and lawfully and in particular will not be processed unless (a) at least one condition in schedule 2 is met and (b) in the case of Sensitive Data at least one condition in schedule 3.
  • Schedule 2 – consent is given or some legal obligation to process data (tax returns, law enforcement etc.)
  • Schedule 3 – *Explicit* consent is given.

• It’s open to discussion how 2 & 3 differ but 3 requires positive action.
Principles 2, 3 & 4.

• 2\textsuperscript{nd} principle
  • Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.
  • Data can’t be collected “just in case it’s useful”

• 3\textsuperscript{rd} principle
  • Personal Data should be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is collected.
  • Often broken without thinking – questions regarding marital status when joining a library etc.

• 4\textsuperscript{th} principle
  • Personal data should be accurate and where necessary kept up to data
  • More tricky than it sounds!
5th Principle

- Personal data processed for any purpose or purposes should not be kept for longer than it is necessary for that purpose or those purposes.

- But how long is enough?
  - Financial data needs to be kept for 7 years for auditing.
  - Civil actions can be issued six years after any event.
  - (Common advice is that emails should be kept for 7 years …)
  - University Exam results might be held indefinitely.
  - CCTV data is routinely deleted after one month
    (this has implications for FOI)

- Procedures for data deletion must be rigorous & specified
  (including deletion of backed up data)
DPA question

• Outline the main principles of the DPA. An itemised list is not required – **full credit will be given for answers which provide a summary of the act.**

• The local council issue a questionnaire to all residents asking their opinions on replacing the existing waste disposal system with wheeley bins. As part of the questionnaire, they in addition ask questions about age, occupation, whether you are home owner or not and your sexuality.

• **Comment on whether such a questionnaire might breach the DPA and discuss the appropriateness of each question listed above.**
Revisiting an old question . . .

In order to seek help, you visit a friendly professor during his office hours. The professor decides he needs a cup of tea and so after welcoming you, excuses himself. You notice his laptop is unlocked and you can see the first page of the resit paper your dim-witted friend is about to take. Your friend is highly anxious and will be thrown off the course if he fails.

1. Discuss briefly how the following factor into any possible outcome:
   - Computer Misuse Act
   - Data Protection Act
   - Freedom of Information

2. What should you do according to:
   - Utilitarian Ethics
     As part of your answer, provide a short description of utilitarianism.
The useful programmer

• A small firm hires a recent graduate to develop a novel algorithm for intelligently selecting adverts for an e-commerce site
• Part of the work is designing the website so that the generated adverts are positioned in an eye catching manner
• As part of his contract, he is required not to write similar software for any competitor for the next 12 months
• The developer leaves the company after two years and is employed to work for a rival company who release their own version of the e-adverts

• The original firm wishes to sue both the programmer and the rival company

What options does the firm have?
More detail

- The programmer is found to suffer from mild dyslexia
- This is not a problem since he has learnt to write code and then use a debugger to correct important things like function calls and variables
- Comments are often misspelt (but who reads those?)

Does this change the chances of success for the firm?
Cloudbox

- An (absent minded) work colleague goes on holiday without sharing an important group report which needs to be submitted next week. The latest version is stored on the colleague’s personal cloudbox account. Cloudbox is a cloud based storage system which uses passwords to control access.

- Since Cloudbox is beyond the reach of your IT department, you suspect that there is nothing you can do. However, another colleague knows that the absent colleague always uses their children’s birthdays as passwords and all the children have FriendFace accounts. It seems likely that you should be able to get the group report after all as long as the children haven’t restricted access to their FriendFace pages.

- With reference to the Computer Misuse Act or any other relevant UK law, comment on whether or not there are any legal or ethical issues involved in using FriendFace to find the children’s birthdays in order to guess the right password.
CloudBox Part 2

- The group report contains sensitive commercial information. Unfortunately Cloudbox is hacked and the report shared with commercial rivals. With reference to any relevant UK law, comment on who is responsible in this situation (i.e. might face civil action from your employers or criminal investigation from the authorities).
A shopping list for revision

- CMA
- DPA
- Intellectual Property
  Copyrights versus trademarks versus patents
- Employment law
  Redundancy, unfair dismissal, basic rights & equality law
- Contract work
- The internet
  an awareness of how international boundaries affect UK law
- Ethics and ethical reasoning
  (i.e. do you know the difference between right and wrong?)
Best of luck with *all* your exams!