# Professional, legal, ethical and social issues

## 1- Overview

The work presented here aims to:

- Instil a professional attitude towards the application of computer technology.
- Provide an appreciation of the law as it relates to computing.
- Introduce methods for the rational resolution of the ethical problems.
- Ensure awareness and encouragement deliberation of the relationship between computer technology and society.

In doing this we will cover work related to:

- Professionalism – in particular professional bodies such as the British Computer Society and the Institution of Engineering and Technology.
- Ways in which your profession decides what actions are appropriate and inappropriate through codes and standards, computer law, and ethical decision making.
- Risks and threats in the field you are studying – crime, privacy and security, and safety critical systems.

## 2 – Professionalism

A professional is someone who belongs to a professional body. When you graduate, and people begin to treat you as a professional because you hold a qualification in your field which has a professional body attached to it, people will expect you to have developed a certain level of expertise and to do things competently, be responsible , and trustworthy.

Professional bodies are the guarantors of your professionalism relating to the responsibility and trust which can be placed on you.
In the United Kingdom the British Computer Society exists for computing professionals and the Institution of Engineering and Technology exists for engineering professionals. In the United States of America the Association of Computing Machinery exists for computing professionals and the Institution of Electrical and Electronic Engineers exists for engineering professionals.
For business professionals the Chartered Institute of Marketing and the Chartered Institute of Management Accountants exist.

Your degree course might be accredited by one or more of the following;

- British Computer Society – for exemption from membership examinations and listing on the register of Chartered Information Technology Professionals.
- Institution of Engineering and Technology – for exemption from membership examinations.
- Engineering Council – for listing on the register of Chartered Engineers.

The British Computer Society:

*The Chartered Engineering Institution for Information Systems Engineers*

The British Computer Society
1st Floor, Block EASY
North Star House
North Star Avenue
Swindon SN2 1FA

http://www.bcs.org
bcshq@hq.bcs.org.uk

Royal Charter 1984 –
*To promote the study and practice of Computing and to advance knowledge therein for the benefit of the public*

The Institution of Engineering and Technology:

*Represents the professions of Electrical, Electronic, Manufacturing and Systems Engineering*

Institution of Engineering and Technology (IET)
Savoy Place
London
WC2R 0BL

http://www.theiet.org
postmaster@theiet.org

*The IET was formed from the Institution of Electrical Engineers (IEE) and the Institution of Incorporated Engineers (IIE) in the spring of 2006*

The Engineering Council:

*ECUK regulates the engineering profession in the UK by licensing engineering institutions to put suitably qualified members on the ECUK's Register of Engineers*

Engineering Council UK
10 Maltravers Street
London
WC2R 3ER

http://www.engc.org

*ECUK's mission is to set and maintain realistic and internationally recognized standards of professional competence and ethics for engineers, technologists and technicians, and to license competent institutions to promote and uphold the standards*

3 – How do professional bodies decide what acts are appropriate and inappropriate?

Your profession decides what actions are appropriate and inappropriate through:

• Codes of conduct, codes of practice and standards. •
Computer law. • Ethical decision making.

## 3.1 - Codes of conduct, codes of practice and standards

Professional bodies will always create codes of conduct and codes of practice.

The British Computer Society code of conduct outlines what is expected as a level of govern professional conduct, professional integrity, that you as a professional pay due heed to the public interest, that you are faithful to your employer and professional field, it alsos your technical competence and impartiality.

A code of good practice refers to how competent you are. The British Computer Society code of practice insists that you pay due attention to the personal requirements of not just yourself or your clients but also those people who might be working for you. The code of practice outlines that you pay due heed to the organization and management issues involved in your work, how you should undertake contract work and pay attention to privacy, security and integrity. The code of good practice covers system development, system implementation and elements of live systems.

International standards can also govern your professional activities. There are many international standards on quality management and quality assurance, the functional safety of electronic systems, and the security of information management systems. Many more standards exist.

## 3.2 – Computer law

In most countries there is a considerable body of law that can apply to computer professionals –

• Contract law. •
Intellectual property law. •
Data protection law. •
Computer misuse law. •
Computer evidence.

If you intend to set yourself up in business you should become familiar with contract law. The most important thing to point out is that the ownership of intellectual property of something you developed depends very much on your role when you developed it. The key phrase is *“I did it in the course of my employment”* – if you develop something in the course of your employment the ownership generally belongs to your employer. If you do something as a contractor, invariably the ownership belongs to you – you have not been employed; you have been brought in and to develop something.

If you are producing computer software with the intent of licensing the software to whoever commissioned it then you own the software. If you produce a piece of bespoke software then, unless you explicitly state in the contract that you intend to

license the software, whoever commissioned it has paid you for, and therefore owns, what you have developed.

Contractual duties which you cannot avoid are:

- Fidelity – dealing honestly and faithfully with people.
- Confidence – how you respect the confidences that are given to you.
- Culpability – the fact that you could be taken to court if you are negligent.
- You CANNOT contract out of reasonable liabilities.

Intellectual property law centers on two main moral rights. The right of patternity, the right to be recognized as the person who created something. And the right of integrity, the right not to have your work tampered with by someone else. Copyright protects original works, sound recordings, and typographical layouts. Copyright lasts for 70 years after the death of the person who created it. In the case of a computer generated work, where the authri cannot die, copyright expires 50 years after the work's creation. Patents protect work for 20 years. Patented ideas are generally novel and not obvious; the important thing to remember is that if you patent something you are expected to use it. In the UK a design right for designs such as printed circuit board layouts is recognized.

There are many statutes of data protection law; because of this it is difficult to distil general principles from these many statutes. The most important thing to remember is that the subject of personal data has the right to view and correct that data. Personal data should be accurate, adequate – sufficient for its purpose, relevant, and kept up to date. Personal data should not be kept for any longer than is necessary.
All appropriate technical and organizational measures should be taken against unauthorized or unfair processing of personal data and against accidental loss or destruction of personal data. For computer data you should make sure that:

- You have appropriate backups of the data.
- You take appropriate security measures to secure the data.

Computer misuse law refers to unauthorized access and unauthorized modification. Unauthorized access of systems, programs, and data is unable while unauthorized modifications through editing and deleting are forbidden. It has been recognized that, through the use of computers, it is possible to commit a crime in a country without actually being present in that country. Modern legislation can now state that it is irrelevant if you are in the country where the crime took place as long as it can be proved that you were responsible for the crime.

Computer evidence concerns what evidence is permissible in a court of law. Evidence may be invalidated if it is viewed after the event. An example of this is if you view log files with an editor after an intrusion, this will invalidate the logs as evidence as it is supposed that they might have been altered after the intrusion. Under normal circumstances specialists were brought in to follow audit trails back to the place of the attack. Amateurs could invalidate evidence or unwittingly tip off perpetrators.

## 3.3 – Ethical decision making

In discussing ethical decision making the areas which we will cover are:

• It is not just about deciding what is right and what is wrong. • Moral systems and principles. • Stakeholder analysis. • Six useful tests.

Ethics is not just about what is right and what is wrong. Scientists and engineers are generally not very good at explaining their work or justifying their actions in non technical terms. We can become absorbed in the technicalities to the point that it becomes so complicated that we cannot explain things in simple terms. When things go wrong and you are responsible in some way the public may seek assurance from you that the technical decisions which were taken paid due heed to the interests of the public. It is crucial that technologists can provide clear and understand justifications for their motives, decisions, and actions.

A way of convincing people that you have their best interests in mind is by citing moral systems. Citing moral systems and principles can help to provide assurance that one's motives, etc. were of good intent. It is important to remember that even though these moral systems and principles have sound foundations not everybody will be re-assured by such references.

A stakeholder analysis approach is a more organized approach. Stakeholder analysis can help you to arrive at sound decisions and provide justifications. Any person, group or organization that could be affected by the decision is a stakeholder.
Stakeholders are not always easy to identify, some are only affected very.
Stakeholder analysis tabulates the alternative decisions and the stakeholders, noting the effect of each alternative on each stakeholder eg very good, good, neutral, bad, or very bad.

Six tests useful which you can apply if you are presented with some kind of dilemma are:

- The Golden Rule – how would you like it if what you are offering to do was done to you?
- The legality test – is what you are forcing to do legal? • The smell test – do you have that feeling in your stomach that it's right or that it's wrong?
- The parent test – would you tell your parents that you are planning to do this? • The media test – how would you defend this on television? • The market test – is the solution that you have come up with so good that you should think about selling it?

## 4 – Case Study

The details of the case study are outlined below, ask yourself the questions:

• What should you do now? •
What should you have considered and done?

### Case Study - “Free and Easy Feedback”

• As a part of your project you create a website. •
You ask your fellow students to give you feedback on the usability of your website via an online questionnaire. • You store all the feedback, unencrypted, along with the name of the person who supplied it in a file in your personal filespace.
• In a free-text box for general comments at the end of your questionnaire one, very thoughtful, responsive states - *“The reason I found the font and background colors difficult to distinguish might be due to my dyslexia”.*

• Six months after you have left university you receive an angry e-mail from the responsive who had stayed on for further study and was now standing for the sabbatical post of President of the Students' Association. • A fellow candidate is distributing election material alluding to the responsive's dyslexia.
• The response is adamant that the only way the information could have been obtained was through the response submitted to your website questionnaire.
• You did not release the personal information.

## 5 – Case Study Answers

What should you do now?

• Apologise – be aware that you are accepting responsibility, but under these circumstances you are quite right to accept responsibility.
• Don't just delete the data; your filespace has been hacked so report it to identify the culprit; don't try to investigate it yourself.

What you should have considered:

• Data protection law •
Stakeholder analysis • Six useful tests

What should you have done?

• Not asked for names – in this case it is unnecessary to know everyone's name. •
Put a clause in to say that you are not responsible for the data – this may be but could inform everyone who submits data that they shouldn't regard what they are submitting useful as being held in confidence. • State up front what you are going to do with the data.

## 6 - Risks and threats in the field you are in

Risks and threats in the field you are in include:

- Computer crime.
- Privacy.
- Security.
- Safety critical systems.

Computer crime costs industry billions of pounds each year. Crime can be broken down into the categories of theft, piracy, espionage, fraud, and sabotage. Theft, plain and simple, involves stealing or taking another's property. Piracy is more common than straight theft. Piracy involves stealing potential revenue and is a criminal offence often involving copyright or patent violation.
Espionage is the stealing of secrets, the acquisition of confidential information. Fraud is deceitfully gaining an advantage, whether it is financial or otherwise. Sabotage is deliberately damaging a system to reduce the effectiveness of the system.

Privacy in computer systems refers to personal data and surveillance and the growing public opinion that too much information is known about us without our knowledge. Personal data is used in consumer databases, health databases, profiling – work relating to data mining and so on, and identity theft. The information about you may possibly be sold unknown to other organisations. Surveillance techniques can be used to gather information about you. Satellite and street cameras are everywhere in society, the websites which you view can be tracked, and even the use of your mobile phone can be monitored.

Computer security can be increased by:

- Verification of identities – how you check that someone is who they say they are.
- Authentication of messages – offer that, if you buy something, you really enter into the deal with the provider.
- Encryption of data – making sure what you send can not be interpreted by inappropriate people.
- Access controls – different levels of access for different user groups.
- Audit trails – tracking back through logs to try and track down where a particular intrusion or attack came from.
- Risk analyses – these should be done at the start of a project to work out what the ultimate risk is.

Safety critical systems are illustrated via two examples.

### Therac-25

The Therac-25 was a new version of a radiation therapy machine with more software control

- Between June 1985 and January 1987 overdoses of radiation were given to six people.
- Three of them died.

The causes of this failure were:

- Poor safety design - lack of safety interlocks, in the previous version hardware interlocks were used – these were removed as it was felt that the controlling software was adequately safe. • Software errors - insufficient testing and debugging. • Inadequate reporting and investigation of accidents. • Overconfidence in using software to replace the hardware interlocks.

Ariane 5

- In June 1996, 40 seconds after initiation of its flight sequence, at an altitude of about 3700m, the Ariane 5 rocket veered off its flight path, broke up and exploded.

- The cause was an internal variable related to the horizontal velocity exceeding the maximum value that a 16-bit integer could hold.
- This software was, in fact, unnecessary for Ariane 5 but necessary in its predecessor, Ariane 4. • It had been retained in the inertial reference system of Ariane 5 for reasons of reasons commonality.

To summarise –

We have looked at what it means to be a computing professional
- What a professional is and the role of professional bodies

We have considered the main branches of law that affect the practice of computing • Contracts, Intellectual Property, Data Protection, Computer Misuse and Computer Evidence

We have examined methods for the resolution of ethical problems
- Moral systems, stakeholder analysis and the six useful tests

We have studied some examples of the relationship between computer technology and society • Crime, privacy, security, risks and threats