Ethics Summary

* Ethical behaviour - *“a set of principles of right conduct or a theory or a system of moral values”*
* Doing the right thing according to standards set by society
* Moral/ethical codes vary at all levels from social groups through organisations up to national levels

Computer Ethics

* a system of moral standards or values used as a **guideline** for computer users
* needed to stop the current technology products from being exploited.

Ethical vs legal behaviour

* Society must enact laws to enforce ethical behaviour
* Impossible to legislate against all possible instances of wrongful behaviour
* the fast pace of technological change means legislation often struggles to keep up with new problems
* The law cannot categorize all ethical requirements

Professional Ethics

* British Computer Society (BCS) is the main professional body for IT professionals in UK
* BCS has a Code of Conduct that all its **members** are expected to follow
* Four main areas (encompassing 17 rules in all)
  + **You make IT for everyone**
  + **Show what you know, learn what you don’t**
  + **Respect the organisation or individual you work for**
  + **Keep IT real. Keep IT professional. Pass IT on**

Professional Ethics (At Brunel)

* “Any research that involves human participation, the collection or study of their data, organs and/or tissue, and that is carried out on Brunel University premises and/or by Brunel University staff or **Brunel University students** under the supervision of Brunel University staff requires **ethical** approval.” (Brunel University research ethics committee, 2005, p. 3).
* Need to conform to BCS code
* Also advise following guidelines from British Psychological Society (BPS, 2004). Specifically regarding:
  + **Consent**
  + **Withdrawal**
  + **Confidentiality**

Legal Issues

* **Computer crime**
  + **Computer Misuse Act (1990)**
* **Protecting personal data**
  + **Data Protection Act (1998, 2018)**
  + **GDPR**
* **Intellectual property**
  + **Copyright**
  + **Patents**

Computer Crime

**Theft**:

* particularly of data and software

**Hacking:**

* Any action that results in unauthorised access to a system with the aim of causing damage or data theft
* Write or use ready-made programs to break into a computer with the intent to steal, damage, modify or monitor data within the system

**Spamming**:

* unsolicited emailing; can disrupt or disable networks

**Denial of service attack**:

* an attempt to make a machine or network resource unavailable to its intended users

**Sniffing**:

electronic eavesdropping on electronic data transmissions; encryption vital to ensure security (e.g. HTTPS)

**Identity theft:**

The fraudulent acquisition and use of person’s private identifying information, usually for financial gain

* + Phishing – fake (albeit credible) requests for confidential data
  + Skimming – details are stolen from magnetic strip or RF tag of a card
  + Shoulder surfing – direct observation of details e.g. being entered/displayed

Computer Misuse Act (CMA) (1990)

* Made it illegal to (attempt to) make unauthorised access or changes to computer material
* Act defines three specific offences:
  + Sect 1: Unauthorised access to computer material
  + Sect 2: Unauthorised access with intent to commit or facilitate commission of further offences
  + Sect 3: Unauthorised modification of computer material (amended see next slide)
* Sections 35 to 38 of Police and Justice Act (2006) contains some [amendments](http://www.legislation.gov.uk/ukpga/2006/48/part/5/crossheading/computer-misuse)
* Section 3 offence is now defined as:
  + *Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.*
  + Most notably, section 3A states that it is an offence to:
  + *supply or offer to supply any article believing that is it likely to be used to commit, or to assist in the commission of, an offence*
* Following the phone hacking scandal, now moves to redefine smart phones as “computers” under the Act

Privacy (Data Protection Act (1994, 1998))

* the ability of an individual/group to stop data or information about themselves from becoming known to people other than those whom they choose to give access
* Data can be sold on to third parties
* Data can be combined from different sources to build a profile of greater complexity than that originally visualized
* Data might be inaccurate, or become so over time
* To counter these and other issues the UK introduced the Data Protection Act (1994, 1998)
* 8 key principles (edited for brevity):

1. Personal data should be processed fairly and lawfully and only if necessary
2. Personal data shall be obtained for one or more specified purposes, and not processed further for other purposes
3. Personal data should be adequate, relevant and not excessive
4. Personal data should be accurate and kept up to date
5. Personal data should not be kept for longer than is necessary for the original purpose
6. Personal data shall be processed in accordance with the rights of data subjects under this Act
7. Appropriate technical and organisational measures shall be taken against unlawful processing, accidental loss, destruction or damage of personal data
8. Personal data should not be transferred to a country outside of the EU unless they ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

* Applies to data held
  + On computers or in computer-readable format
  + Manually (if in structured form)
  + Example: medical and educational records
* Under 1994 Act, Data Subjects had the basic right to know what data was held about them
* New rights of data subjects under 1998 Act:
  + To know nature of data held
  + To know why and how it is to be processed
  + To know to whom it may be disclosed
  + To have copies of the data, subject to nominal fee (£10)
  + To object to and prevent processing of data if damage/distress would be caused
  + To claim compensation for damage caused by breach of the Act

Data Protection Act (2018)

* The Data Protection Act updates our data protection laws for the digital age. It received Royal Assent on 23 May 2018.
* Digital technology has transformed almost every aspect of our lives in the twenty years since the last Data Protection Act was passed.
* The new Data Protection Act:
  + makes our data protection laws fit for the digital age in which an ever increasing amount of data is being processed
  + empowers people to take control of their data
  + supports UK businesses and organisations through the change
  + ensures that the UK is prepared for the future after we have left the EU

General Data Protection Regulation (GDPR)

* a regulation in the European Union (EU) law on data protection and privacy for all individuals within the EU and the European Economic Area.
* It came into action on 25 May 2018.
* It specifies how businesses and public sector organisations can handle the information of their customers.
* It gives more rights and control over their information.
* The GDPR applies to processing carried out by organisations operating
  + within the EU;
  + outside the EU that offer goods or services to individuals in the EU.
* The GDPR does not apply to
  + certain activities including processing covered by the Law Enforcement Directive;
  + processing for national security purposes;
  + processing carried out by individuals purely for personal/household activities.

(What information does the GDPR apply to?)

* Personal data
  + any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
  + applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria
  + Sensitive personal data
    - Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
    - Genetic data, biometric data for the purpose of uniquely identifying a natural person.
    - Data concerning health or data concerning a natural person's sex life or sexual orientation.
* Personal data relating to criminal convictions and offences **are not included.**

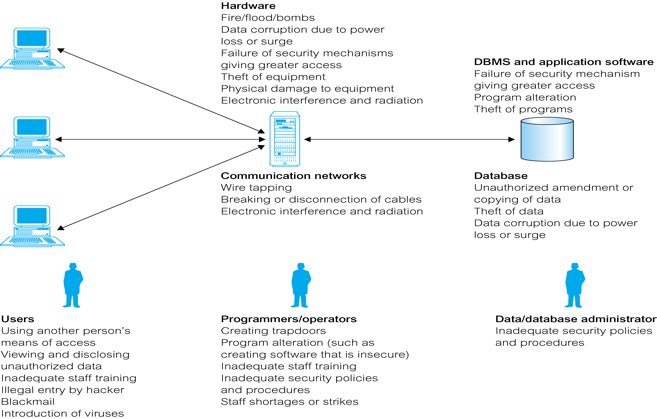
Personal data should be

* processed lawfully, fairly and in a transparent manner in relation to individuals;
* collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
* adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
* accurate and, where necessary, kept up to date;
* kept in a form which permits identification of data subjects for **no longer** than is necessary for the purposes for which the personal data are processed.
* processed in a manner that ensures appropriate security of the personal data.

Data Security

The mechanisms that protect the data against intentional or accidental threats

* Security can be breached in different ways
  + Theft and fraud
  + Loss of confidentiality – rights of organisation to secrecy
  + Loss of privacy – rights of control over personal data
  + Loss of integrity – damage or loss of data
  + Loss of availability – system down-time
* A security breach can be catastrophic to an organisation leading to
  + Lost revenue
  + Unexpected repair costs
  + Damaged reputation
  + Legal liability
  + Loss of IP / competitive advantage
* Central to BCS Code of Conduct
  + **Public interest** refers to privacy
  + **Professional competence and integrity** refers to the need to keep up with technological developments and relevant legislation
  + **Duty to relevant authority** requires you to maintain confidentiality



Reducing security risks

* **Authorisation**
  + **Access controls** govern not only access to data but how it can be used
  + Access determined by **authentication** process (e.g. user name and password)
  + User access controlled by the system administrator
  + **Privileges** specify which objects (e.g. folders/files, DB tables) a user needs to read/modify in order to do their job
    - Granting of unnecessary privileges should be avoided
* **Backup and recovery**
* Making regular copies data and (in DB system) the log-file (transaction history) that contains information about all updates to the database.
* Backup window: The time during which the backup can occur
* backing up volatile data during busy periods can cause integrity problems.
* If possible scheduled out of normal operating hours
* Full back-ups are time/space consuming are often done periodically with incremental or differential back-ups
* **Encryption**
  + Use of an algorithm that encodes data using an encryption key, whereby data can only be decoded (made readable) with the decryption key
  + Brute force methods can ‘crack’ 64-bit encryption key quite quickly. 128-bit or longer keys should be more reliable for the foreseeable future
* **Firewalls**
  + Server/router based software that controls external access to the local network
* Install a firewall and anti-virus software
* Install anti spy/malware tools
* Install updates
* Choose strong passwords and don’t share
* Encrypt sensitive data
* Make regular data back-ups
* Wipe all data before disposal/resale

Intellectual Property

* Intellectual property (IP) is intangible property created by an individual or organisation
  + Literary works, music, video, art, designs, inventions and trademarks
* Often a large amount of time, effort and funding is involved in the development of IP
* It is called “intellectual” property because it is the product of human imagination, creativity, and inventiveness
* The producer needs to be protected from others profiting from their hard-work without their consent
* Protecting your intellectual property makes it easier to take legal action against anyone who steals or copies it, with an aim of making profit
* Two main types of protection:
  + Copyright [for literary works, art, music, films ,sound recordings, web content
  + Patents[invention and products, e.g. machines and machine parts, tools, medicines)

1. Copyright

* Comes into effect automatically - protects the expression or manifestation of an idea (not the idea itself).
* It covers
  + Traditional documents like books, music articles, movies/TV
  + Computer software, databases, designs and multimedia
* Copyright (UK) normally extends beyond the author’s lifetime. Some exceptions:
  + Sound records and broadcasts – 50 years
  + Published editions (typographical arrangement) – 25 years
* Authors may license others to produce copies, often in return for *royalties*
* Whilst software is automatically copyright, this does not prevent others from writing their own code to implement the same ideas (reverse engineering)

1. Patent

* A more powerful means of protecting IP
  + A patent protects your **invention** and lets you take legal action against anyone who makes, uses, or sells your invention without your permission
* **Protects** the idea behind an invention
* The ideas should be original and not obvious
  + A new, useful and inventive step
* Patents are published, thus benefiting public knowledge
* There are clear boundaries defining what can be patented
  + Software is not (usually) patentable
  + Artistic creations, mathematical models, plans, schemes or other purely mental processes cannot be patented