FACTFILE:
GCE DIGITAL TECHNOLOGY

UNIT A21: INFORMATION SYSTEMS

Rewarding Learning

ICT and Legislation

Learning Outcomes

Students should be able to:
Describe the main features of the following legislation:

- The Data Protection Act;
- The Copyright, Designs and Patents Act;
- The Computer Misuse Act;
- Understand and apply how each piece of legislation may impact on organisations, their employees and members of the public.
- Explain the ethical considerations around automated decision making, online censorship, monitoring of personal behaviour, artificial intelligence and the capture, storage and analysis of personal information.

Content in ICT and Legislation

- ICT Legislation.
- Ethical considerations.

ICT Legislation

The main ICT legislation includes:

- Data Protection Act.
- The Copyright Designs and Patents Act.
- Computer Misuse Act.

Data Protection Act

The increased volume of information stored on computers meant there was a need to control what was stored in the interests of protecting individual personal data. This law was designed to protect individual personal data and it was defined as having eight principles. These include:

- Personal data should be processed fairly and lawfully with the consent of the data subject.

- Personal data should be used for the specified purpose only.
- Personal data should be adequate and relevant for its intended purpose.
- Personal data should be accurate and up to date.
- Personal data should not be kept for longer than necessary.
- Personal data should be processed in accordance with the rights of the data subject.
- Personal data should be held securely, with no unauthorised access.
- Personal data should not be transferred outside the EU.

The law also specified the roles of key people as:

Key Person	Outline of Role
Data Subject	The individual who is the subject of the personal data
The Commissioner	Responsible for enforcing the Act Promoting good practice from those people responsible for processing personal data Making the general public aware of their rights under the Act
The Data Controller	The person in a company who is responsible for controlling the way in which personal data is processed

The impact of Data Protection legislation

The main aim of this legislation is to protect the rights of individuals who have data held on them by organisations. Under its terms the organisation is held responsible for the security, accuracy and conditions of use of the data it holds. Organisations that do not comply with the terms of the DPA can be prosecuted. It is therefore critical that all data-using organisations have procedures in place to ensure that data is held securely, that its accuracy is maintained and that it is used by the organisation correctly.

Organisations should ensure that procedures should be in place to ensure that data stored is accurate and up-to-date, for example through the use of validation and verification procedures. Ensuring that data is up-to-date may involve regular contact with data subjects, asking them to verify currently held details on a regular basis. Organisations also need to ensure that data stored is consistent with the requirement that data must only be used for the originally designated purpose.

They must also ensure that measures are in place to protect the integrity and physical security of the data held. This will involve implementing various security measures, including: physical access, system access, firewalls, back-ups, etc.
The organisation must also provide training to ensure that staff is aware of data protection issues and of their personal responsibility for ensuring the terms of the act are complied with.

The Copyright Designs and Patents Act

This law was designed to protect the "intellectual property" rights of those individuals and organisations that create and produce material based on original ideas. Material of this kind includes books, articles, music, films, software, etc. Software piracy is a concern as this involves the illegal copying, modifying or downloading of software. By doing this they are avoiding the price of buying the software. It can also be the 'theft' by one company of the ideas and methods of other ICT companies.

The impact of Copyright Designs and Patents legislation

Software piracy can take many forms such as individual users using the Internet to copy a piece of software to their own computers without permission to professional criminals making copies in bulk and selling them through illegal outlets.
The software industry believes that there are two negative effects of piracy. Firstly, it results in higher prices for those customers who are buying software legally and secondly, it discourages software houses from being innovative in creating new software.

When organisations that use computer networks to purchase a piece of software, they also purchase a software licence for one or more users. They are then legally permitted to distribute the software to that number of users. If the organisation wants more users to access the software, then they have to pay for more licences.

For an organisation to enforce this law they have

a responsibility to ensure that all employees are aware of the terms of the Act and the consequences of being in breach of it. The organisation must also carry out audits on the software that it uses and monitors who has access to that software.

Organisations must fully comply with Licensing agreements and must control access to the software. Employees should only be allowed to have authorised software on their PCs. Organisations should also ensure that unauthorised software, perhaps brought from home or downloaded from the Internet, is not permitted in the workplace.

Computer Misuse Act

This act was designed to prevent computer crimes involving unlawful access to information systems or data files. The act states that unauthorised access to computer material is an offence, unauthorised access with intent to commit or facilitate commission of further offences is also offence and unauthorised modification of computer material is a further offence. It identifies specific crimes such as deliberately planting viruses in a computer system hacking into someone's computer system.

The impact of Computer Misuse legislation

Whilst it is unlikely that a legitimate organisation would deliberately breach the terms of this Act, individual employees may use company resources to hack into other systems. If it were shown that the organisation was negligent in taking steps to prevent this, it could be held partly liable for the actions of its employees. The organisation should put policies should be in place to ensure that employees are aware of the terms of the Act and the consequence of being in breach of it This would include an "Acceptable Use" policy including organisational disciplinary procedures.

Computer use by employees should be audited regularly and suspect access activity be fully investigated, through examining parts of the system that have been accessed by different employees at specified times. Implementing a username and password system will mean access to different areas of the system is tightly controlled meaning employees should have only access rights that are necessary for the completion of their work.

Ethical Considerations

Ethics are an accumulation of values and principles that address questions of what is good or bad in human affairs. Ethics searches for reasons for acting or refraining from acting; for approving or not approving conduct; for believing or denying something about virtuous or vicious conduct or good or evil rules.

The proliferation of digital communication, content and connectivity provides a number of the ethical challenges.

What are the ethical issues?

Many of the ethical issues that face IT professionals involve privacy.

- Should you read the private e-mail of your network users just because you can? Is it OK to read employees' e-mail as a security measure to ensure that sensitive company information isn't being disclosed? Is it OK to read employees' e-mail to ensure that company rules (for instance, against personal use of the e-mail system) aren't being violated? If you do read employees' e-mail, should you disclose that policy to them? Before or after the fact?

- Is it OK to monitor the Web sites visited by your network users? Should you routinely keep logs of visited sites? Is it negligent to not monitor such Internet usage, to prevent the possibility of pornography in the workplace that could create a hostile work environment?

- Is it OK to place key loggers on machines on the network to capture everything the user types? What about screen capture programs so you can see everything that's displayed? Should users be informed that they're being watched in this way?

- Is it OK to read the documents and look at the graphics files that are stored on users' computers or in their directories on the file server?

The key point is that this is not about legislation. A company may very well have the legal right to monitor everything an employee does with its computer equipment. But what about the ethical aspects of having the ability to do so?

For example, as a network administrator or security professional, you have rights and privileges that allow you to access most of the data on the systems on your network. You may even be able to access encrypted data if you have access to the recovery agent account. What you do with those abilities depends in part on your particular job duties (for example, if monitoring employee mail is a part of your official job description) and in part on

your personal ethical beliefs about these issues. In looking at the list of privacy issues above, it is easy to justify each of the actions described. But it is also easy to see how each of those actions could "morph" into much less justifiable actions. For example, the information you gained from reading someone's e-mail could be used to embarrass that person, to gain a political advantage within the company, to get him/her disciplined or fired, or even for blackmail.

The slippery slope concept can also go beyond using your IT skills. If it's OK to read other employees' e-mail, is it also OK to go through their desk drawers when they aren't there? To open their briefcases or purses?

Examples of ethical dilemmas

What if your perusal of random documents reveals company trade secrets? What if you later leave the company and go to work for a competitor? Is it wrong to use that knowledge in your new job? Would it be "more wrong" if you printed out those documents and took them with you, than if you just relied on your memory?

What if the documents you read showed that the company was violating government regulations or laws? Do you have a moral obligation to turn them in, or are you ethically bound to respect your employer's privacy? Would it make a difference if you signed a nondisclosure agreement when you accepted the job?

IT and security consultants who do work for multiple companies have even more ethical issues to deal with. If you learn things about one of your clients that might affect your other client(s), where does your loyalty lie?

Then there are money issues. The proliferation of network attacks, hacks, viruses and other threats to their IT infrastructures have caused many companies to "be afraid, be very afraid." As a security consultant, it may be very easy to play on that fear to convince companies to spend far more money than they really need to. Is it wrong for you to charge hundreds or even thousands of dollars per hour for your services, or is it a case of "whatever the market will bear?"

Another ethical issue involves promising more than you can deliver, or manipulating data to obtain higher fees. You can install technologies and configure settings to make a client's network more secure, but you can never make it completely secure. Is it wrong to talk a client into replacing their current firewalls with those of a different manufacturer, or switching to an open source operating system – which changes, coincidentally, will result in many more billable hours for you – on the premise that this is the answer to their security problems?

The question "Is it ethical?" must be answered by each individual IT professional.

Unlike older, more established professions such as medicine and law, most ethical issues that IT and security professionals confront have not been codified into law, nor is there a standard mandatory oversight body, such as the national medical association or bar association, that has established a detailed code of ethics.

However, the question of ethical behaviours in the IT professions is beginning to be addressed. Voluntary professional associations such as the Association for Computing Machinery (ACM) have developed their own codes of ethics and professional conduct, which can serve as a guideline for individuals and other organizations.

Digital Theft and Copyright Violation

One of the biggest challenges that digitizing everything from music to movies has created has been the ease with which these assets can be stolen and shared at little or no cost and with no apparent penalties.

For example, is it okay for a friend to give you a digital copy of a song they purchased? Most people would say Yes. However, if you had spent time and money and had used your talent to record an album and discovered that it was shared without you being paid anything, would that be okay?

Privacy

What about the impact of the explosive growth of connected devices and what it means for our privacy? We expose a significant amount of data online through searches and social media posts. Many of our clicks generates to data that is sold to marketers and other third parties.