OCR A Level Computer Science

Your notes

5.1 Computing Related Legislation

Contents

- The Data Protection Act 1998
- The Computer Misuse Act 1990
- The Copyright Design & Patents Act 1988
- The Regulation of Investigatory Powers Act 2000

Your notes

The Data Protection Act 1998

What is The Data Protection Act?

- The **Data Protection Act** (DPA) is a law that protects personal data from being misused
- Examples of personal data would include
  - Name
  - Address
  - Date of Birth
  - Race
  - Religion
- Most people that store personal data has to follow the Data Protection Principles although there are a few exemptions:
  - **Domestic purposes** – if you only use personal data for such things as writing to friends and family or taking pictures for your own enjoyment, you are not subject to the DPA
  - **Law enforcement** – the Police investigating a crime is not subject to the DPA. E.g. if someone has been suspected of a crime they can't request to see the evidence about them
  - **Intelligence services processing** – personal data processed by the intelligence services (eg MI5) is not covered by the DPA

The Data Protection Principles

Principle	How does it affect a company?	Example
1. Personal data must be fairly and lawfully processed	A company has to be clear about what personal data they wish to collect and what they want to use it for.	A school can request personal data to be able to call guardians in an emergency.

2. Personal data must be collected for specified and lawful purposes	A company cannot use personal data for any purpose other than what they stated originally. They also cannot pass this data on without permission.	A company asks for a phone number to call regarding delivery but then uses it to market new products.
3. Personal data must be adequate, relevant and not excessive	A company cannot request personal data that they do not need right away.	A bank cannot ask for their customer's previous trips when opening an account.
4. Personal data must be kept accurate and up to date	If a company holds personal data that is wrong or out of date then you have a right to have it corrected or deleted.	If a bank has a customer's old address then they will not be able to send up to date statements.
5. Personal data will not be kept for longer than is necessary	A company must delete personal data once they no longer have a need for it.	If a customer closes their account the company must delete their data.
6. Personal data must be processed in line with people's rights	If requested a company must provide a customer with all the personal data they hold on them.	A hospital has to give a patient's full records if requested by the patient.
7. Personal data must be held securely	A company is required to make sure that personal data they keep is secured (usernames and passwords) and is backed up to prevent accidental loss.	A company could make external backups on the cloud.
8. Personal data must not be transferred to countries outside the European Economic Area unless those countries have similar data protection laws	A company cannot send personal data outside the European Economic area unless the country in question has been deemed by the European Commission to provide a good level of protection of personal data.	A company cannot send its data to China because they are not deemed to have adequate Data Protection.

Your notes

Examiner Tip

- When you get a question asking to explain the principles make sure you explain them and not just state them.
  - Example: *Personal data must be fairly and lawfully processed which means that companies must collect personal information with a lawful reason to have the data*
- OCR are also aware that the law is constantly changing especially in regards to DPA therefore answers will be accepted that use an interpretation of the law based on when the specification was set (2015) or when the examination was sat.
  - E.g. you can include GDPR


Your notes

Actions Companies Must Take

- Companies can face extremely large fines if they are found to be in breach of the **Data Protection Act**
- Companies must appoint a member of staff as their **Data Controller**. They will then be responsible for making sure that the principles of the **Data Protection Act** are not breached and to keep in communication with the **Information Commissioner**
- The company must put in place physical or digital security measures to prevent the data from being accessed without consent
- The company should make sure that they train their staff to abide by the principles
- Companies must send a copy of the subject's data if a **Subject Access Request (SAR)** is received. This copy must be sent securely after the company has verified the identity of the subject

Rights of an Individual Under the DPA

Under the Data Protection legislation, data subjects have the following rights with regards to their personal information:

- To be informed about the collection and the use of their personal data
- To access personal data and supplementary information
- To have inaccurate personal data rectified, or completed if it is incomplete
- To be forgotten in certain circumstances
- To restrict processing in certain circumstances
- To data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services
- To object to processing in certain circumstances

- To automated decision making and profiling
- To withdraw consent at any time (where relevant)
- To complain to the Information Commissioner


Your notes

Case Study

British Airways fined £20m over GDPR Breach

"British Airways (BA) has been fined £20 million by the UK's data protection authority over data security failings which enabled unauthorised access to be obtained to personal and payment card information relating to more than 400,000 of its customers." - External link to Pisent Masons article

Things that British Airways could have done to prevent the breach:

- Making sure that employees have multi-factor authentications on their log-ins
- Using Role-based controls that allow different users to be assigned different permissions
- Having a form of efficient and effective security monitoring
- Regularly penetration testing and fixing any issues that occur promptly

These are all deemed good practice and would have likely either prevented the attack or enabled British Airways to spot the breach themselves as opposed to being told about it by a third party.

Your notes

The Computer Misuse Act 1990

What is the Computer Misuse Act?

- The **Computer Misuse Act (CMA)** concerns the malicious use of computers. The act was originally created to make sure that computer **hacking** was covered within the law
- It has been updated regularly to ensure it remains relevant
- Features can be deployed to minimise the threat from unauthorised access for example **digital signatures** or certificates
- **Firewalls** can be used to prevent external people accessing the system. They are key in preventing **DoS** or **DDos** attacks

Primary Offences Under the CMA

The Computer Misuse Act has 3 primary offences:

1. **Unauthorised access** to computer materials
   E.g. If a student finds out a teacher's password and then accesses their computer and opens their files.
2. **Unauthorised access with intent** to commit further offences
   E.g. If the student finds out a teacher's password and then accesses their computer with the intent to increase their marks on their last test result.
3. **Unauthorised modification** of computer files
   E.g. If the student finds out a teacher's password and then accesses their computer and increases their mark on their last test result.

The consequences of each offence are worse depending on whether it's offence 1, 2 or 3 with each offence being punishable with time in prison.

Case Study

Two individuals were sentenced under the Computer Misuse Act for Theft of Data

- The Information Commissioner's Office (ICO) has led the successful prosecution of 2 individuals for violating the CMA by stealing personal information to make scam calls
- Kim Doyle who is now a former employee of the RAC was found guilty of transferring personal data to to accident claims firm without permission

- This included data such as road traffic accident data, names, phone numbers and registration numbers
- She pleaded guilty to conspiracy to secure unauthorised access to computer data, and selling unlawfully obtained personal data
- Kim Doyle and William Shaw have been handed an 8 month prison sentence which was suspended for 2 years

Your notes

Examiner Tip

- You need to make sure that when answering a question on the Computer Misuse Act that you not only describe the law but relate it to the relevant scenario asked
  - How does the Computer Misuse Act affect the company in the scenario?
  - What are the consequences of the actions taken?

Worked Example

"The Computer Misuse Act means that computer users are criminalised for simply trying to learn how systems work"

Discuss whether or not you agree with this statement.

9 marks

How to answer this question:

- Describe your knowledge of the Computer Misuse Act
- Mention the three main offences
- Apply to a scenario, in this case the question hasn't given us a full scenario so we can use our own
- Keep the argument balanced, once you've spoken about one side, then speak about the other
- Then write your conclusion and use your own opinion

Answer:

Example answer that gets full marks:

The Computer Misuse Act (CMA) is a provision for securing computer material against unauthorised access or modification to the system.

Under the CMA there are three main offences that you can be prosecuted for; The unauthorised access to a computer system, the unauthorised access to the computer system with intent to make changes and unauthorised access to the computer system and making changes.

Users can still investigate how computer systems work; they would just need to get authorisation before doing so. For example you could ask the owner of the computer system to allow access first or you could create a virtual computer system and use this to investigate.

The CMA could however be broken by accessing an email account of somebody without permission. Ultimately users need to make sure that they are aware of the law when accessing any computer system.

In conclusion I disagree with the statement "The Computer Misuse Act means that computer users are criminalised for simply trying to learn how systems work" as users are able to educate themselves on the details of the CMA easily online and therefore should know the consequences of accessing a computer system without the right authorisation. There are plenty of online platforms, programs and systems that are accessible to access virtually and would not be in breach of the CMA.


Your notes

Your notes

The Copyright Designs & Patents Act 1988

What is the Copyright Designs & Patents Act?

- This protects the **intellectual property** of an individual or a company
- It makes it illegal to copy, modify or distribute software or other intellectual property without the relevant **permission**
- If **original work** is original, **copyright** will be automatically applied and will not expire until 25 - 70 years from the death of the creator depending on the type of work
- If an individual believes that their work has been copied it is their responsibility to take action under the **Copyright Designs and Patents Act**
- Many sites online offer free downloads of copyrighted **software/videos** which prevents the intellectual copyright holder from earning their income on the work they have created
  - E.g. If someone downloaded videos from Netflix and shared them with others, they would be breaching the act
- The act covers videos and audio where **peer-to-peer streaming** prevents a copyright owner from receiving an income

What is Prohibited Under the Copyright, Designs & Patents Act?

Primary Breaches:

- Copying an original work
- Issuing the copy of the original work to the public
- Renting/lending the copy of the original work to the public
- Performing, showing or playing the original work in public
- Making an adaptation of the original work

Secondary Breaches:

- Importing a copy of original work
- Possessing or dealing with a copy of the original work
- Providing means to make copies of the original work

- Permitting the use of premises for making copies of the original work
- Provision of props/equipment for a performance of a copy of the original work

Your notes

Case Study

Ed Sheeran Vs Marvin Gaye (External link to bbc.co.uk)

- A case was brought against Ed Sheeran about his song 'Thinking Out Loud'
- Ed Sheeran won his case which ruled that he did not copy 'Let's Get It On' by Marvin Gaye whilst composing 'Thinking Out Loud'
- The heirs of Gaye's co-writer argued that Sheeran owed them money for infringement of copyright
- Sheeran said that if he was found guilty he would give up his music career
- The songs were said to have a similar chord progression but it was argued that these are the base of all modern songs and should be free to use
- Sheeran won a high court battle in London in 2022 over the copyright of his 2017 song 'Shape of You'
- In 2015 Gaye's heirs won a $5.3m judgement from a lawsuit claiming that Robin Thicke's 'Blurred Lines' copied Gaye's 'Got to Give it Up'

Examiner Tip

- Make sure that you specify that the Copyright Design and Patents Act covers original work and is automatically applied from the creation of the work, then talk about what this means for the distribution of the work. For example:
  - *The work was protected by the Copyright Designs and Patents act when it was created. Therefore if anyone wishes to distribute it they have to gain the owner's permission, if they just posted it to the internet then this would be in breach of the act.*
- Also when referring to the name of the act, ensure you use its full name (The Copyright, Designs and Patents Act). It's not called the Copyright Act. If you use a shortened version it may cost you marks in the exam


Your notes

The Regulation of Investigatory Powers Act 2000

What is the Regulation of Investigatory Powers?

- The Regulation of Investigatory Powers Act (RIPA) legislates as to how organisations can monitor electronic communications
- The **RIPA** covers **investigation**, **surveillance** and **interception** of communication by public bodies
  - E.g. MI6 can legally wiretap online conversations in the interests of national security provided that a warrant has been issued
- Certain actions require government approval
- Different organisations have different limits on what they can do (GCHQ is amongst those that have most freedom)
- The Act enforces **internet service providers (ISPs)** and mobile phone companies to give up information on request from an authorised authority and to ensure that their networks have sufficient hardware installed to facilitate surveillance about a person
- This Act is particularly controversial as its powers also extend to small agencies like local councils
- Some people feel that the Act is an invasion of **privacy** or that it is used improperly
- There have been examples of this Act being used for reasons other than monitoring criminal or terrorist activities including monitoring cockle fisherman, fly tippers, and even a family to work out whether they lived in the catchment area of a local school

Rights & Impact on Organisations

With the increase in criminal and terrorist activities on the internet this act allows the Police and other public bodies to:

- Demand ISPs to provide access to a customer's communications
  - This means that ISPs have to implement hardware and software which facilitates the surveillance of digital communications
- Allows mass surveillance of communications
- Demands access to be granted to protected information
  - Businesses have to provide access to digital communications or data when asked for

- They have to implement hardware and software solutions that facilitates the storage of digital communications
- Allowing monitoring of an individual's internet activities
- Prevents the existence of such interception activities being revealed in court


Your notes

Case Study

British Councils used RIPA to secretly spy on public (External link to theguardian.com)

- In 2016 an investigation was completed after councils were given permission to carry out more than 55,000 days of covert surveillance over 5 years which included people walking dogs, feeding pigeons and fly-tipping
- A freedom of information request has found that 186 local authorities, two-thirds of those that responded, used RIPA to gather evidence by secret listening devices, cameras and private detectives

Examiner Tip

- When you are asked to describe the RIPA you need to specify the technical terms "surveillance" and "communication" and don't generalise them
- **Surveillance** is the use of technology to gather information on people, and the **communication** is done electronically