GCST

1.5.1 COMPUTING RELATED LEGISLATION

TOPIC WISE EXAM QUESTIONS

ANSWERS

A-LEVEL OCR

4	(e)	(i)	• Copyright Designs and Patents Act Any two from: • Gives the author (the programmers) ownership/copyright of the photographs • …no need to apply // this is automatic • Others cannot use/distribute // can be prosecuted/fined for using/distributing… • …without permission • Permission can be granted / bought / licenced	3	Must be full name of Act for MP1 FT for versions of Copyright or nothing for MP2-6
4	(e)	(ii)	• Ask permission of **author / photographer / owner** • Use images marked as copyright free (e.g. Creative Commons Licence) • Purchase (licence to use) image	2	Do not accept just "ask permission"
7*			**Mark Band 3 – High Level (9-12 marks)** The candidate demonstrates a thorough knowledge and understanding of The Regulation of Investigatory Powers Act (RIPA) 2000. The material is generally accurate and detailed. The candidate is able to apply their knowledge and understanding directly and consistently to the context provided. Evidence/examples will be explicitly relevant to the explanation. The candidate is able to weigh up both sides of the argument which results in a supported and realistic judgement covering the benefits and drawbacks of the Act. This is well balanced. There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated. **Mark Band 2 – Mid Level (5-8 marks)** The candidate demonstrates reasonable knowledge and understanding of The Regulation of Investigatory Powers Act (RIPA) 2000; the material is generally accurate but at times underdeveloped. The candidate is able to apply their knowledge and understanding directly to the context provided although one or two opportunities are missed. Evidence / examples are for the most part implicitly relevant to the explanation. The candidate makes a reasonable attempt to come to a conclusion showing some recognition of benefits and/or drawbacks. This may not be well-balanced, covering one side significantly more than the other, although both sides will be present. There is a line of reasoning presented with some structure. The information presented is in the most part relevant and supported by some evidence. **Mark Band 1 – Low Level (1-4 marks)** The candidate demonstrates a basic knowledge of The Regulation of Investigatory Powers Act (RIPA) 2000; the material is basic and contains some inaccuracies. The candidate makes a limited attempt to apply acquired knowledge and understanding to the context provided. The candidate provides nothing more than unsupported	12 AO1.1 (2) AO1.2 (2) AO2.1 (2) AO3.3 (3)	*The following shows example content that may form part of a candidate's answer. It is not intended to be an exhaustive resource, nor should a candidate be expected to specifically cover any particular amount of this.* **Knowledge (AO1)** • Implements additional rights regarding surveillance / monitoring of individuals and acquisition of communications data • Provides the right for many organisations (including the Police and security services) to do this. • Purpose is to detect crime and defend national security (e.g. terrorism, public disorder) • Gives access to individuals' private communications, such as emails, text messages, phone calls, Internet history. • Some people feel this is an invasion of their privacy **Application (AO2)** • Monitoring can be carried out by far more organisations than just the Police and Security services – for example, local councils, the pension regulator and the Environment Agency are all able to use surveillance or request data about individuals. • If files are encrypted, the Act gives powers to force the handover of keys (from individuals or organisations) with a 2 year prison sentence possible on refusal. • Wide ranging powers have allowed Police and Security services to intercept criminals' communications and stop / disrupt crime. **Evaluation (AO3)** • In the modern world, it is important that Police and Security services are given the power to deal with electronic communications in this way. Many crimes (e.g. terrorism) can be detected and stopped before they occur, making the public safer. • However, some say that it is now a "snooper's charter", with more organisations using their powers for minor offences such as detecting those lying about their address to get children into a better school or fly-tipping. • Many communication tools (e.g. WhatsApp) now include end-to-end encryption by default so that messages cannot be divulged by the organisation because they do not have access to it. Other encryption tools include plausible deniability.

GCST

2022

	(e)		• Copyright assigned to owner of video automatically on creation • Makes it illegal to copy/distribute videos **as your own/without permission** • Copyright holder can ask for their work to be removed from the streaming platform • Membership/licence gives subscribers the agreement to view videos • Which may restrict their use (e.g. to whom it is shown or geographical location from which it is accessed).	2

2021

4	(a)		**Mark Band 3–High Level (7-9 marks)** The candidate demonstrates a thorough knowledge and understanding of legislation including the Computer Misuse Act. The material is generally accurate and detailed. The candidate is able to apply their knowledge and understanding directly and consistently to the context provided. Evidence/examples will be explicitly relevant to the explanation. The candidate provides a thorough discussion which is well balanced. Evaluative comments are consistently relevant and well-considered. There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated. **Mark Band 2-Mid Level (4-6 marks)** The candidate demonstrates reasonable knowledge and understanding legislation including the Computer Misuse Act; the material is generally accurate but at times underdeveloped. The candidate is able to apply their knowledge and understanding directly to the context provided although one or two opportunities are missed. Evidence/examples are for the most part implicitly relevant to the explanation. The candidate provides a sound discussion, the majority of which is focused. Evaluative comments are for the most part appropriate, although one or two opportunities for development are missed.	9 AO1.1 (2), AO1.2 (2), AO2.1 (2), AO3.3. (3)	AO1 Computer Misuse Act is legislation aimed at criminalising unauthorised access to a computer system Three stages: Unauthorised access to a computer system Unauthorised access with intent to commit further offences Unauthorised modification of computer material Punishable by up to twelve months in prison and an unlimited fine. AO2 Computer users who investigate how systems work require authorisation in order to not break the Act. Examples such as changing a social media post on a friend's mobile phone potentially breaks all three sections of the Act. Investigation of systems can break the Act without intent, e.g. by changing server logs because of their actions. Users must be aware of the Act (as with any other law) in order to be responsible. AO3 Material available online (e.g. self study videos) that explain how systems work and teach without the need to investigate using unauthorised access. Investigating systems that you own yourself or have authorisation to access does not break the law. Systems are offered to users with strict conditions attached and investigation is not a legitimate excuse for breaking the law. Ethical / white hat hackers will not break this law because they have authorisation. Grey and black hat hackers will break Computer Misuse Act.

5		Mark Band 3–High Level (7-9 marks) The candidate demonstrates a thorough knowledge and understanding of the regulation of the Internet; the material is generally accurate and detailed. The candidate is able to apply their knowledge and understanding directly and consistently to the context provided. Evidence/examples will be explicitly relevant to the explanation. The candidate provides a thorough discussion which is well-balanced. Evaluative comments are consistently relevant and well-considered. There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated. Candidate has used appropriate technical terminology throughout. There are few if any spelling errors or errors of grammar. Mark Band 2 –Mid Level (4-6 marks) The candidate demonstrates reasonable knowledge and understanding of the regulation of the Internet; the material is generally accurate but at times underdeveloped. The candidate is able to apply their knowledge and understanding directly to the context provided although one or two opportunities are missed. Evidence/examples are for the most part implicitly relevant to the explanation The candidate provides a reasonable discussion, the majority of which is focused. Evaluative comments are for the most part appropriate, although one or two opportunities for development are missed. There is a line of reasoning presented with some structure. The information presented is in the most part relevant and supported	9 AO1.1 (2) AO1.2 (2) AO2.1 (2) AO3.3 (3)	Anyone can put content onto the Internet. It can be hard to track down who put information up. People can make untrue claims or present biased information. There are certain crimes that have originated because of the internet (e.g. phishing and pharming) Other crimes have found new avenues through the internet (e.g. drugs, obscene materials etc.) Laws have been written to take into account the internet (e.g. RIPA in the UK). Traditional laws still apply to the Internet. Governments can apply laws in their jurisdictions… ..but may not be able to enforce them if content is from outside their country. It can be hard to track people down if they actively try to hide their identity. Regulation whilst difficult on the internet may be to some extent desirable. Education is important – teaching people about the risks of using the internet. Content is available to people of all ages and vulnerabilities.
7	a	<table><tr><th>Scenario</th><th>Computer Misuse Act</th><th>Copyright Design and Patents Act</th><th>Data Protection Act</th></tr><tr><td>A bank accidentally publishes customers' account details on its website.</td><td></td><td></td><td>✓</td></tr><tr><td>Someone downloads a pirated version of a piece of software that users would ordinarily have to pay for.</td><td></td><td>✓</td><td></td></tr><tr><td>Someone writes and distributes a virus.</td><td>✓</td><td></td><td></td></tr></table> 1 Mark per row	3 (AO2.1)	
	b	- Sets out to empower/ limit the extent... - to which public bodies … - can use technological surveillance.. - This can include monitoring internet activity - Electronic communications - And forcing users to hand over encryption keys (1 per - , max 3)	3 (AO1.2)	

6			**Mark Band 3–High Level (9-12 marks)** The candidate demonstrates a thorough knowledge and understanding of computing related laws and modern issues that fall under them. The material is generally accurate and detailed. The candidate is able to apply their knowledge and understanding directly and consistently to the context provided. Evidence/examples will be explicitly relevant to the explanation. The candidate is able to assess the extent to which the law is able to keep up with changes in technology. There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated. **Mark Band 2-Mid Level (5-8 marks)** The candidate demonstrates reasonable knowledge and understanding of computing related laws and modern issues that fall under them; the material is generally accurate but at times underdeveloped. The candidate is able to apply their knowledge and understanding directly to the context provided although one or two opportunities are missed. Evidence/examples are for the most part implicitly relevant to the explanation. The candidate makes a reasonable attempt to come to a conclusion as to whether the law is able to keep up with changes in technology.	12 AO1.1 (2) AO1.2 (2) AO2.1 (3) AO3.3 (5)	Points may include but aren't limited to: **AO1 Knowledge and Understanding** Laws that regulate technology include: the Data Protection Act… …which regulates how personal data is stored. The Computer Misuse Act… …which regulates unauthorised access. The Copyright and Patents Act… …regulated intellectual property. Regulation of Investigatory Powers Act… …Regulates how government agencies can use IT for surveillance **AO2 Application** Computer Misuse Act is harder to enforce with the increased use of DDoS attacks (often involving unwitting participants). The Internet of things is likely to make such attacks even more common place. People are connecting to the internet in new ways using mobile networks/public Wi-Fi making attacks potentially difficult to track. Films/Music etc. are being shared in new ways. Streaming is common – often this is legitimate but the global nature of it can bring licensing issues into play. Fast internet speeds, peer to peer and the dark web all contribute to making piracy more prevalent and harder to track. Digital watermarking can be used to track piracy. End to end encryption makes government monitoring of communications trickier.
			There is a line of reasoning presented with some structure. The information presented is in the most part relevant and supported by some evidence. **Mark Band 1-Low Level (1-4 marks)** The candidate demonstrates a basic knowledge of computing related laws and modern issues that fall under them; the material is basic and contains some inaccuracies. The candidate makes a limited attempt to apply acquired knowledge and understanding to the		**AO3 Evaluation** May conclude that although technology develops quickly the laws are broad enough to cover all eventualities. Alternatively, may conclude that people are always looking for ways of using technology to access loophole in the law / to avoid detection. Look for a well-reasoned conclusion. Could decide either for or against but should be backed up with examples.

GCST EXTRA

1			• Customer has the right to see the data and to ask for it to be corrected if wrong so that they are not responsible for incorrect data • Data must be lawfully collected so that customer rights are not flouted • Data can only be accessed by/changed by authorised people so that malicious alterations are not made • Authorised people must be notified to the DPR so that they are accountable • Data is only used for the specified purpose so that junk mail is not encouraged • Data collected should not be excessive so that irrelevant data is not stored • Data should be accurate and up to date so that customers are not held responsible for goods they have not bought • Data should not be kept longer than necessary so that customers can leave an organisation • Data should be protected by adequate security measures so that people with malicious intent cannot gain access • Data should not be transferred out of the EU so that data remains subject to DPA. (1 per bullet, max 7)	7	Not just 'Cannot pass on or sell data' Accept Access to DPR if not satisfied with responses from company
2	a		**Four from:** □ Ensure only relevant data is held about them [1] □ It is kept up to date [1] □ It is accurate [1] □ Must not be held longer than necessary. [1] □ Employees are given access to their data [1] □ Data must be kept securely [1] □ Data must not be passed on to 3rd parties without permission. □ Data must not be passed outside the EU [1]	4	

If you found this useful, drop a follow to help me out!

THANK YOU!

GCST

GCSECOMPUTERSCIENCETUTOR.COM