1(a) Government bodies have been given additional powers under the Regulation of Investigatory Powers Act.

State **three** additional powers that this law gives to some government bodies.

1 ---

---

2 ---

---

3 ---

[3]

(b) An investigative firm wants to start investigating cyber security issues. As part of their new roles, employees will be accessing personal data. In order to facilitate this, all employees are enrolled on a course about the Data Protection Act.

Identify **three** principles of the Data Protection Act.

1 ---

---

2 ---

---

3 ---

[3]

2 The Regulation of Investigatory Powers Act (2000) has been described as both a vital legal tool to ensure the public's safety and an attack on an individual's freedoms.

Evaluate the purpose and use of the Act.

You should include:

- the additional powers given under the Act
- to whom these powers are given
- the perceived benefits and/or drawbacks of the Act.

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

[12]

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

3 The Copyright Designs and Patents Act 1988 applies to all videos that are streamed.

Explain how this act applies to the videos.

[2]

4 * Many technologists predict that in the future, shops on the high street will use facial recognition to identify customers before they walk into a shop.

Discuss the possible benefits and drawbacks of technology being used in this way.

You should refer to the following in your answer:

- The benefits and drawbacks to both the customers and businesses
- Moral and ethical issues
- Legal issues

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

[9]

5 * *"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]

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

6 * “When it comes to government electronic surveillance, if you have nothing to hide, you have nothing to fear.”

Discuss whether or not you agree with this statement. You should include:

- To what extent the UK government is able to monitor electronic communications of its citizens
- Technical measures citizens can take to help prevent their communications being monitored.

[9]

7 A number of laws govern the use of computers.

Describe the purpose of the Regulation of Investigatory Powers Act.

[3]

8 * *'Technology is changing too quickly for the law to keep up.'*

Discuss to what extent you agree with the statement above. In your discussion you should explain which laws regulate the use of technology and how advancements in technology have made the laws difficult to enforce/implement.

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

[12]

9 The Government Communications Headquarters (GCHQ) is responsible for monitoring communications in order to keep the UK secure. A large part of its job involves trying to break into encrypted messages.

GCHQ has to operate within the law. Describe how the law allows GCHQ to monitor communications.

[2]

END OF QUESTION PAPER

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

Question			Answer/Indicative content	Marks	Guidance
1	a		1 mark per bullet to max 3: • Allows for mass surveillance of communications • Allows the **monitoring** of an individual's internet activities/history • Allows covert surveillance to be carried out • Can demand access to protected data • Can demand that ISPs/businesses give access to customer communications/history • Can demand that ISPs/businesses install equipment that facilitate surveillance • Can demand that encryption keys are handed over // force individuals to decrypt data • Can keep existence of searches and what found private in court	3	Allow other suitable answers relating to examples of other types of surveillance e.g. CCTV, directed surveillance. MP4 relates to password protected data or accessing data protected under the DPA Examiner's Comments There were a number of candidates who could not accurately name one additional power.
	b		1 mark per bullet to max 3: • Data must be processed **fairly/ lawfully** • Data must be **adequate/ relevant/ not excessive** • Data must be **accurate** and (where necessary) **up to date** • Data must **not be retained for longer than necessary** • Data can only be **used for the purpose** for which it was collected • Data must be **kept secure** • Data must be **processed in accordance with people's rights** • Data must not be transferred outside of the EU without adequate protection // to other countries who do not have equivalent data protection laws	3	Accept: Right to see their own data/change if incorrect Examiner's Comments This was generally well answered and candidates showed good understanding of the Data Protection Act (DPA) principles.
			Total	6	

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

Question			Answer/Indicative content	Marks	Guidance
2			**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	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

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

Question			Answer/Indicative content	Marks	Guidance
			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 assertions. Any conclusion, if present, will be almost entirely one-sided. The information is basic and communicated in an unstructured way. The information is supported by limited evidence and the relationship to the evidence may not be clear. **0 mark** No attempt to answer the question or response is not worthy of credit.		"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. Examiner's Comments Responses to this question were varied, some candidates showed a clear understanding of the powers and to whom they are given. Some were aware of the powers but focused on the police or security services in their response. Some went off track, talking about other countries. In general this was not answered well and candidates tended to have a one sided view of the act.
			Total	12	
3			• 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	Examiner's Comments Most candidates were able to gain 1 mark for this question, but few went on to gain a second mark.
			Total	2	

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

Question			Answer/Indicative content	Marks	Guidance

4			**Mark Band 3–High Level**
			(7-9 marks)
			The candidate has weighed up benefits and drawbacks of the technology and has applied the moral, legal and ethical issues to both the customer and the business; 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 will have come to a fully justified conclusion.
			
			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 has weighed up benefits and drawbacks of the technology. They will have explored some of the moral, legal and ethical issues but they may not be equally spread across both the customer and the business; 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 will have come to a conclusion although they may not fully justify it.
			
			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
			(1-3 marks)
			The candidate identifies some of the benefits and drawbacks, though they have probably shown little consideration of the legal, ethical and moral issues; the material is basic and contains some inaccuracies.
			The candidate makes a limited attempt to apply acquired knowledge and
				9
				(AO1.1)
				(2)
				(AO1.2)
				(2)
				(AO2.1)
				(2)
				(AO3.3)
				(3)
					<u>Knowledge:</u> **Benefits**
					Customer:
					
					• Personalised offers
					
					Business:
					
					• Targeted adverts
					• Able to track movement habits of customers
					• Provide more personalised shopping experiences.
					
					Drawbacks
					Customer:
					
					• Personal intrusion
					• Invasion of privacy
					• Pressured selling
					
					Business:
					
					• Cost of infra structure
					• Viewed as invading personal privacy
					
					Moral and Ethical issues
					
					• Violation of civil liberties
					• Recording people on the street who are not going into the shop
					
					Legal issues:
					
					• under data protection laws the shop would need to
					  ◦ Keep any data recorded secure
					  ◦ Personal data should be accurate and up to date
					
					<u>Application:</u>
					Benefits
					Customer:
					
					• Personalised experience will lead to more convenient shopping trips
					• Staff will give personalised service
					
					Business:
					
					• Tracking movement of customers means able to identify best opening times
					• Tracking customers around shop allows better analysis of popular products

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

Question	Answer/Indicative content	Marks	Guidance
	understanding to the context provided. The candidate may not reach a recognisable conclusion. *The information is basic and communicated in an unstructured way. The information is supported by limited evidence and the relationship to the evidence may not be clear.* **0 marks** No attempt to answer the question or response is not worthy of credit.		• Use of modern technology will make the shop be seen as forward thinking. **Drawbacks** Customer: • Customers may not want to be "pressured" meaning they decide not to shop there anymore. • Tracking data could be hacked and used by criminals Business: • Extra hardware costs may lead to higher prices/competitors undercut them. • Customers who feel their privacy has been invaded may "vote with their feet" **Moral and Ethical issues** • Abuse of civil liberties could damage reputation of shop **Legal issues:** • Shop may need to add extra software to blur out faces of non-customers • Shop will need to spend more money on data protection compliance, leading to higher costs. Evaluation: Benefits • Increased revenue from directed sales offset extra costs from hardware/legal obligations • Improved reputation through use of modern technologies may attract more customers Drawbacks: • Loss of customer base due to customers unhappy with "pushy techniques" • Poor public opinion from invasive advertising puts new customers off. Examiner's Comments Candidates were assessed on the quality of their extended response in this question.

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

Question			Answer/Indicative content	Marks	Guidance
					Most candidates understood the basic concept of storing personal details being a violation of customers civil liberties. Few candidates had a balanced discussion and focused too heavily on the negative aspects of this system therefore being restricted to a mid-level mark.
			Total	9	

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

Question			Answer/Indicative content	Marks	Guidance
5			**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. 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 (1-3 marks)** The candidate demonstrates a basic knowledge of legislation including the Computer Misuse Act; the material is basic and contains some inaccuracies. The candidate makes a limited attempt to apply acquired knowledge and understanding to	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.

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

Question			Answer/Indicative content	Marks	Guidance
			the context provided. The candidate provides a limited discussion which is narrow in focus. Judgments if made are weak and unsubstantiated. The information is basic and communicated in an unstructured way. The information is supported by limited evidence and the relationship to the evidence may not be clear. 0 marks No attempt to answer the question or response is not worthy of credit.		
			Total	9	

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

Question			Answer/Indicative content	Marks	Guidance
6			**Mark Band 3–High Level (7-9 marks)** The candidate demonstrates a thorough knowledge and understanding of electronic communication monitoring techniques and the social and legal impact of this. 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 electronic communication monitoring techniques and the social and legal impact of this; 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. 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 (1-3 marks)** The candidate demonstrates a basic knowledge of electronic communication monitoring techniques and the social and legal impact of this; the material is basic	9 AO1.1 (2) AO1.2 (2) AO2.1 (2) AO3.3 (3)	AO1 Encryption means that data is scrambled so that if it is intercepted, it cannot be understood. Requires the use of a key to decrypt. Symmetric encryption uses on key for encrypt/decrypt and so key exchange is problematic. Asymmetric encryption uses different keys (public and private) so no need to exchange keys. Regulation of Investigatory Powers Act (RIPA) gives authorities the power to compel disclosure of encryption keys AO2 Encrypted messages cannot be read by outsiders without the key RIPA gives Police the power to insist on users decrypting messages / handing over the key to allow reading of messages. Many messaging services already include end-to-end encryption by default Use of VPNs to re-route traffic and attempt to escape monitoring possible The ending of encrypted data shows that two parties are passing information they want to keep secret. Techniques like steganography can be used to his the existence of encrypted data. AO3 Monitoring communication runs the risk of revealing secret but non-illegal communications Restricting encryption means that secure sites (eg banks) may struggle to function Legislation (RIPA) already ensures that communications can be monitored if there is just cause Routine monitoring runs the risk of false-positives However, will reduce risk of illegal activities being co-ordinated (e.g. terrorism, drug trafficking).

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

Question			Answer/Indicative content	Marks	Guidance
			and contains some inaccuracies. The candidate makes a limited attempt to apply acquired knowledge and understanding to the context provided. The candidate provides a limited discussion which is narrow in focus. Judgments if made are weak and unsubstantiated. The information is basic and communicated in an unstructured way. The information is supported by limited evidence and the relationship to the evidence may not be clear. 0 marks No attempt to answer the question or response is not worthy of credit.		
			Total	9	
7			– 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)	Examiner's Comments Many candidate responses lacked the technical terminology appropriate for this level of study. The terms 'surveillance' and 'communication' were used too generically. Candidates need to make it clear that the surveillance is technological and the communication electronic.
			Total	3	

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

Question			Answer/Indicative content	Marks	Guidance
8			**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. 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	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. **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. Examiner's Comments Candidates were assessed on the quality of their extended response in this

© OCR 2026. You may photocopy this page.

Created in ExamBuilder

Question			Answer/Indicative content	Marks	Guidance
			inaccuracies. The candidate makes a limited attempt to apply acquired knowledge and understanding to the context provided. The candidate provides nothing more than an unsupported assertion. The information is basic and communicated in an unstructured way. The information is supported by limited evidence and the relationship to the evidence may not be clear. 0 marks No attempt to answer the question or response is not worthy of credit.		question. Many candidates offered a balanced discussion although some were limited in scope i.e. limiting the discussion to one law. Few conclusions were appropriately justified/reasoned leading to many candidates scoring in the mid-level band on this question.
			Total	12	
9			- The Regulation of Investigatory Powers Act (Accept RIPA) - Legislates as to how organisations can monitor electronic communications - Allows interception of communications - Allows them to get communications information from ISP - Allows them to perform surveillance (e.g. key logging) - Certain actions require government approval - Different organisations have different limits on what they can do (GCHQ is amongst those that have most freedom). (1 per -, max 2)	2 AO2.1 (2)	<u>Examiner's Comments</u> Few candidates cited the 'Regulation of Investigatory Powers Act (RIPA)' correctly. Some candidates cited '…monitoring communications' for how the law is applied, which was given in the question therefore, in isolation, this did not gain credit.
			Total	2	

© OCR 2026. You may photocopy this page.

Created in ExamBuilder