1.5 LEGAL, MORAL & ETHICAL · 1.5.1

Computing legislation — Mark scheme

30 marks · spec 1.5.1(a)–(d)

AO key: AO1 = knowledge · AO2 = application · AO3 = reasoned judgements. Accept any valid alternative. Do not award the same point twice.

Q	ANSWER	AO	MARKS
1(a)	Data Protection Act. (1)	AO2	1
1(b)	Computer Misuse Act. (1)	AO2	1
1(c)	Copyright, Designs and Patents Act. (1)	AO2	1
1(d)	Regulation of Investigatory Powers Act (RIPA). (1)	AO2	1
1(e)	1990. (1)	AO1	1

Q	ANSWER	AO	MARKS
2(a)	1 mark each, max 3: processed lawfully/fairly · used only for its specified purpose · adequate/relevant, not excessive · accurate & up to date · not kept longer than necessary · kept secure · not transferred without adequate protection. (3)	AO1	3
2(b)	Request to see the personal data the company holds about them. (1)	AO1	1
2(c)	1 mark each, max 2: passwords / authentication · encryption of personal data · access rights / restricted access · firewalls · physical security · staff training. (2)	AO2	2

Q	ANSWER	AO	MARKS
3(a)	Unauthorised access to computer material (1); unauthorised access with intent to commit a further offence (1); unauthorised modification of computer material (1). (3)	AO1	3
3(b)	2 examples, 1 mark each (tool + how used): keylogger — records keystrokes/ passwords (1); password cracker — guesses/decrypts passwords (1); port scanner · smartcard reader · trojan, etc. (2)	AO2	2
3(c)	Unauthorised modification of computer material. (1)	AO2	1

Q	ANSWER	AO	MARKS
4(a)	Copyright, Designs and Patents Act (1); 1988 (1). (2)	AO1	2
4(b)	1 mark each, max 2: buy/obtain a licence to use the image · use royalty-free / Creative-Commons licensed images · get the creator's permission · commission/ create their own. (2)	AO2	2
4(c)	Regulation of Investigatory Powers Act (RIPA) 2000. (1)	AO1	1

<table>
<tr><th>Q</th><th>LEVELS-OF-RESPONSE MARK SCHEME</th><th>AO</th><th>MARKS</th></tr>
<tr><td>5</td><td>Mark using the levels descriptors below. AO1 (knowledge of RIPA/surveillance), AO2 (application), AO3 (balanced judgement).

<table><tr><th>LEVEL</th><th>DESCRIPTOR</th></tr><tr><td>Level 3 (6–8)</td><td>A balanced discussion with clear arguments for and against, well applied, leading to a justified conclusion. Well structured with accurate use of terminology.</td></tr><tr><td>Level 2 (3–5)</td><td>Arguments on both sides with some development; a conclusion that is partially justified.</td></tr><tr><td>Level 1 (1–2)</td><td>Basic points, largely one-sided, with little development.</td></tr><tr><td>0</td><td>Nothing creditworthy.</td></tr></table>
Indicative content (credit any valid point):
• For: helps catch serious criminals and terrorists; can prevent attacks; lawful oversight; "if you have nothing to hide…".
• Against: invades privacy of innocent people; potential for misuse/abuse of power; weakening encryption harms everyone's security; chilling effect on free expression.
• Application: ISPs forced to fit equipment / hand over data; demanding encryption keys undermines secure communication.
• A reasoned conclusion weighing security against privacy.</td><td>AO1 ×3
AO2 ×3
AO3 ×2</td><td>8</td></tr>
</table>

Total for paper: 30 marks