1.5 Legal, Moral, Cultural and Ethical Issues

OCR H446 · Calculators not allowed · about 100 minutes · Write-in edition

Total Marks

Name: _____ Date: ____ / ____ / _____

Answer ALL questions. Show all your working.

1 Redwood Sports Academy uses a cloud-based system to store data about student athletes, including their medical conditions and performance statistics.

(a) State the UK Act that governs how the academy must handle this personal data, and name the framework it incorporates into UK law. **(2)**

(b) The academy keeps full medical records for athletes who left five years ago, 'in case they are useful in future'. Identify which data protection principle this breaches and explain why. **(3)**

(c) The academy shares an athlete's mental health data with a sponsor, without asking the athlete, to help the sponsor decide whether to fund them. Explain why this is a particularly serious breach of data protection law. **(3)**

(Total for Question 1 is 8 marks)

2 Nadia Hussain runs a small games studio. She has written a new game engine and is deciding how to license it.

(a) Explain the difference between open source and proprietary software licensing. **(3)**

(b) Nadia releases her engine under a Creative Commons Attribution-NonCommercial (CC BY-NC) licence. State what each of the two conditions means for someone who wants to use the engine. **(2)**

(c) A rival developer, Owen Blackwood, copies Nadia's proprietary source code without permission and sells a near-identical game. State the Act that has been broken, identify the right that has been infringed, and state one civil remedy available to Nadia. **(3)**

(Total for Question 2 is 8 marks)

3 Elmswood Borough Council receives a request from a local journalist, Grace Ellison, asking how much the council spent on new laptops last year.

(a) State which Act gives Grace Ellison the right to make this request, and identify the type of organisation this Act applies to. **(2)**

(b) Explain two reasons why the council might legally withhold or redact some of the information Grace has requested. **(3)**

(c) Discuss one benefit and one drawback of the Freedom of Information Act for public sector organisations such as Elmswood Borough Council. **(3)**

(Total for Question 3 is 8 marks)

4 A data centre in Sheffield runs 2000 servers. Each server draws 300 watts of power continuously (24 hours a day).

(a) Calculate the energy used by one server in one day, giving your answer in kWh. **(2)**

(b) Calculate the total energy used by all 2000 servers in the data centre in one day, giving your answer in kWh. **(2)**

(c) Discuss the environmental impact of large data centres such as this one, and evaluate one way this impact could be reduced. **(5)**

(Total for Question 4 is 9 marks)

5 BrightPath Learning, a UK education technology company, wants to sell its revision app in Japan, Saudi Arabia and Germany.

(a) Identify three cultural or legal factors, other than translating the text, that BrightPath Learning must consider when adapting (localising) its app for these markets. **(3)**

(b) Discuss the cultural and ethical challenges of creating 'one size fits all' educational software for a global market, evaluating whether full localisation is always achievable or desirable. **(4)**

(Total for Question 5 is 7 marks)

6 Oakfield University uses an automated plagiarism-detection system that compares every piece of submitted coursework against a global database of previous student work, journal articles and websites, producing a percentage 'similarity score'. A first-year student, Sophie Chen, is placed under investigation after her essay returns a 42% similarity score.

(a) Explain one benefit and one drawback of using automated plagiarism-detection software, from an ethical and cultural perspective, referring to fairness for students. **(3)**

(b) Evaluate whether it is ethical for a university to rely primarily on a percentage similarity score, without human review, to decide whether a student has committed academic misconduct. **(4)**

(Total for Question 6 is 7 marks)

7 Leah Kowalski is a software engineer producing control software for railway level crossings. During testing, she finds a rare timing bug that could, in one specific circumstance, leave a barrier open for an extra two seconds after a train is detected. Her manager tells her to ignore it because the release deadline is in three days and fixing it would cause a delay.

(a) State the name of the UK professional body for IT that publishes a code of conduct for computing professionals, and identify one principle from a typical professional code of conduct relevant to this scenario. **(2)**

(b) Explain why Leah has an individual moral responsibility to act on this bug, even though her manager has told her to release the software as planned. **(3)**

(c) Discuss the options available to Leah and evaluate which course of action best balances her professional, ethical and legal responsibilities. **(5)**

(Total for Question 7 is 10 marks)

8 AutoDrive Motors is trialling a self-driving car on UK roads. In an emergency where a collision is unavoidable, the car's control software must choose between braking hard (risking injury to the passenger) or swerving (risking injury to a pedestrian, Omar Farouk, who has stepped into the road).

(a) Identify who might bear legal and moral responsibility if the car's decision leads to injury, and explain why assigning responsibility is harder than with a human driver. **(3)**

(b) Evaluate the ethical challenges of programming a self-driving car to make decisions in unavoidable-collision scenarios, and discuss whether it is possible to create rules that are morally acceptable to everyone. **(7)**

(Total for Question 8 is 10 marks)

9 A cyber-security researcher, Ryan McAllister, discovers a vulnerability in the software used by a UK hospital trust's patient record system. Without permission, he accesses a live test copy of the system to confirm the vulnerability is real, then emails the hospital IT department describing the flaw. Two months later, having received no response, he publishes full technical details of the vulnerability, including working exploit code, on his personal blog. A criminal group then uses this exploit to access and copy 50,000 patients' medical records, which are later found for sale on the dark web.

(a) For each of the following actions, identify whether Ryan McAllister could be prosecuted under the Computer Misuse Act 1990, and if so, under which section: (i) accessing the test copy of the system without permission; (ii) publishing the exploit code online. **(4)**

(b) Identify which piece of legislation is relevant to the hospital trust's own responsibilities after 50,000 patient records are stolen, and explain what the trust may be required to do as a result. **(4)**

(c) Evaluate whether the ethical practice of 'responsible disclosure' (privately reporting vulnerabilities and giving organisations time to fix them before publishing details) is an adequate solution to balancing the interests of security researchers, organisations and the public. Using this scenario to support your answer, discuss whether current UK legislation, such as the Computer Misuse Act 1990, adequately supports ethical security research. **(9)**

(Total for Question 9 is 17 marks)

Mark scheme · 1.5 Legal, Moral, Cultural and Ethical Issues

Question 1

(a) Data Protection Act 2018 **B1**

(a) UK GDPR / General Data Protection Regulation (oe) **B1**

(a) Answer: Data Protection Act 2018, incorporating the UK GDPR.

(b) Identifies the storage limitation principle (oe) **B1**

(b) Explains that data must not be kept for longer than necessary for the purpose it was collected **B1**

(b) Applies this to the scenario: the athletes have left, so there is no ongoing purpose, so the records should be deleted or anonymised **B1**

(b) Answer: This breaches the storage limitation principle; data has no ongoing purpose once an athlete leaves and should not be retained indefinitely.

(c) Identifies that health data is 'special category data' under the UK GDPR (oe) **B1**

(c) Explains that special category data requires an extra lawful condition, normally explicit consent, before it can be processed/shared **B1**

(c) Explains a consequence/harm, e.g. potential discrimination against the athlete, loss of sponsorship, distress, breach of trust **B1**

(c) Answer: Sharing special category data without explicit consent (or another Article 9 condition) is unlawful and can cause serious harm to the athlete.

Question 2

(a) Open source: the source code is made available and users may view, modify and redistribute it (oe) **B1**

(a) Proprietary: the source code is kept private/hidden and copying, modifying or redistributing it is restricted by the owner (oe) **B1**

(a) Valid comparative point, e.g. open source can be cheaper/more customisable, proprietary can offer more guaranteed support/quality control **B1**

(a) Answer: Open source licences allow access to and reuse of source code; proprietary licences restrict access and reuse to protect the owner's rights.

(b) Attribution: the user must credit Nadia as the original creator (oe) **B1**

(b) NonCommercial: the user may only use the engine for non-commercial purposes, e.g. not sell a product built with it (oe) **B1**

(b) Answer: Attribution = must credit the creator; NonCommercial = may not be used to make money.

(c) Copyright, Designs and Patents Act 1988 **B1**

(c) Infringement of Nadia's copyright / right to reproduce and distribute her own work (oe) **B1**

(c) Valid remedy, e.g. injunction to stop further sales, damages/compensation, account of profits **B1**

(c) Answer: Copyright, Designs and Patents Act 1988; infringement of copyright; remedy such as an injunction or damages.

Question 3

(a) Freedom of Information Act 2000 **B1**

(a) Public authorities/public sector bodies, e.g. councils, government departments, state schools, NHS (oe, any one example accepted) **B1**

(a) Answer: Freedom of Information Act 2000; applies to public authorities.

(b) Valid exemption reason 1, e.g. information is commercially sensitive (ongoing supplier negotiations) **B1**

(b) Valid exemption reason 2, e.g. information contains personal data of named staff, protected under data protection law **B1**

(b) Reference to the process, e.g. a public interest test must be applied to qualified exemptions, or the request must be answered within 20 working days **B1**

(b) Answer: Exemptions may apply for commercially sensitive information or personal data; qualified exemptions are subject to a public interest test.

(c) Valid benefit, e.g. increases transparency and public accountability, builds trust in how public money is spent **B1**

(c) Valid drawback, e.g. significant staff time/cost to process requests, risk of releasing information that harms commercial negotiations **B1**

(c) Balanced comparative or concluding comment linking benefit and drawback **B1**

(c) Answer: Benefit: greater transparency/accountability. Drawback: administrative cost and risk of commercially damaging disclosure. A balance must be struck using exemptions.

Question 4

(a) Converts 300 W to 0.3 kW and multiplies by 24 hours (oe method) **M1**

(a) 7.2 kWh, cao **A1**

(a) Answer: 7.2 kWh

(b) Multiplies answer to (a) by 2000 (ft from a) **M1**

(b) 14400 kWh (ft from a), cao **A1**

(b) Answer: 14 400 kWh (14.4 MWh)

(c) **L1** Basic, undeveloped identification of one or two impacts (e.g. energy use, e-waste) with little or no discussion of reduction methods. **1-2**

(c) **L2** Clear explanation of two or more impacts (e.g. energy use/carbon emissions, cooling water use, e-waste from hardware replacement) with at least one reasonably developed method of reduction. **3-4**

(c) **L3** Sustained, well-developed discussion covering multiple impacts and a clearly evaluated method of reduction, reaching a reasoned judgement about its effectiveness or limitations. **5**

(c) Indicative content:

- High continuous electricity demand contributes to carbon emissions, especially where power is not from renewable sources.
- Cooling systems for servers use large amounts of energy and, in some designs, large amounts of water.
- Frequent hardware replacement/upgrade cycles generate electronic waste (e-waste), some of which contains hazardous materials and is difficult to recycle safely.
- Reduction methods: server virtualisation to reduce the number of physical servers needed; sourcing renewable electricity; locating data centres in cooler climates to reduce cooling energy; reusing waste heat to warm nearby buildings.
- Evaluation: reduction methods often involve upfront cost or practical limitations (e.g. renewable supply is not always available, virtualisation still requires hardware refresh), so impact reduction is a trade-off rather than a complete solution.

(c) Answer: N/A - levels-marked extended response.

Question 5

(a) Valid factor 1, e.g. reading direction/layout (right-to-left text for Arabic) **B1**

(a) Valid factor 2, e.g. colours, symbols or imagery that have different cultural or religious meanings in different countries **B1**

(a) Valid factor 3, e.g. date/number/currency formats, local data protection laws that may differ from UK GDPR, or local content/censorship rules **B1**

(a) Answer: Any three of: reading direction/layout; culturally sensitive colours/symbols/imagery; date, number or currency formats; local data protection or censorship laws.

(b) **L1** Identifies a benefit or challenge of a global platform with limited explanation or evaluation. **1-2**

(b) **L2** Clear discussion of both benefits (e.g. shared access to quality resources, cost-effectiveness) and challenges (e.g. cultural imperialism, censorship conflicts, cost/time of localisation), with a reasoned evaluative judgement about achievability or desirability. **3-4**

(b) Indicative content:

- Benefit: a shared global platform can be cheaper to build and maintain, and can widen access to good-quality educational resources, potentially reducing the digital divide.
- Challenge: exporting content designed around one culture's norms and values risks 'cultural imperialism', imposing assumptions that do not fit other cultures.
- Challenge: content acceptable in the UK (e.g. discussion of certain scientific, religious or social topics) may conflict with local censorship rules or cultural sensitivities elsewhere.
- Challenge: full localisation is costly and time-consuming for a small company, so genuine adaptation for every market may not be commercially achievable.
- Evaluation: a balance is often struck through partial localisation (adapting the most sensitive elements) rather than either a single global version or full bespoke versions for every market.

(b) Answer: N/A - levels-marked extended response.

Question 6

(a) Benefit: consistent, fast detection across a whole cohort supports fairness and deters deliberate academic dishonesty **B1**

(a) Drawback: false positives are possible, e.g. common technical phrases, properly cited quotations, or writing conventions from a student's first language/culture may be flagged unfairly **B1**

(a) Developed point linking to Sophie's case, e.g. a similarity score alone does not distinguish plagiarism from legitimate quotation/paraphrase, so context and human review are needed before judging her **B1**

(a) Answer: Benefit: consistent, scalable, fair detection across all students. Drawback: risk of false positives, especially for legitimately cited or common technical language, which can unfairly disadvantage individual students such as Sophie.

(b) Point that a raw score lacks context/nuance, e.g. it cannot reliably distinguish properly referenced quotation from genuine plagiarism **B1**

(b) Point about due process/fairness, e.g. a student should have the right to explain flagged sections before a judgement is made **B1**

(b) Point recognising the institution's argument, e.g. efficiency/consistency at scale across thousands of submissions **B1**

(b) Evaluative concluding statement, e.g. the score should trigger further human review, not act as an automatic verdict, to be considered ethical **B1**

(b) Answer: It is not fully ethical to rely on the score alone; it should be used as a trigger for human review rather than a final verdict, balancing efficiency with fairness and due process.

Question 7

(a) BCS, The Chartered Institute for IT (oe) **B1**

(a) Valid principle, e.g. members must have due regard for the public health, privacy, security and wellbeing of others **B1**

(a) Answer: BCS, The Chartered Institute for IT; its code of conduct requires members to prioritise public safety and wellbeing.

(b) Explains the potential harm to public safety, given this is a life-critical/safety-critical system **B1**

(b) Explains that a professional's ethical duty of care can override a manager's commercial instruction when public safety is at risk **B1**

(b) Explains a consequence of not acting, e.g. legal/professional liability, loss of public trust, risk of prosecution if harm occurs **B1**

(b) Answer: Because the system is safety-critical, Leah's professional duty of care to protect the public overrides commercial pressure to meet the deadline; failing to act could cause real harm and expose her and the company to liability.

(c) **L1** States one or two options with little explanation or evaluation. **1-2**

(c) **L2** Explains a range of options with some evaluation of which is most appropriate, but the argument may be one-sided or not fully developed. **3-4**

(c) **L3** Sustained discussion of multiple options with a clear, reasoned evaluation leading to a justified recommendation. **5**

(c) Indicative content:

- Options: report the bug formally to senior management/quality assurance in writing; refuse to sign off the release; escalate to a safety regulator such as the Office of Rail and Road; delay release until the fix is made; as a last resort, disclose externally/whistleblow.
- The Public Interest Disclosure Act 1998 offers UK employees legal protection against dismissal for whistleblowing on genuine safety concerns, but this is typically considered a last resort after internal routes are exhausted.
- Documenting concerns in writing protects Leah professionally and creates a record that due diligence was carried out.
- Evaluation: escalating internally first (formally, in writing, to a level above the immediate manager) is usually the most proportionate first step, reserving external whistleblowing for cases where internal escalation fails and the risk to the public is imminent.

(c) Answer: N/A - levels-marked extended response.

Question 8

(a) Identifies at least two possible responsible parties, e.g. the manufacturer, the software developers, the vehicle owner/supervising 'driver', the insurer **B1**

(a) Explains the difficulty: the decision was made by a pre-programmed algorithm rather than a real-time human judgement, so it is unclear whose 'choice' actually caused the outcome **B1**

(a) Valid reference to relevant framework, e.g. the Automated and Electric Vehicles Act 2018 makes insurers primarily liable for incidents while a vehicle is driving itself **B1**

(a) Answer: Responsibility could fall on the manufacturer, developers, owner or insurer; assigning it is harder because the decision was embedded in code in advance rather than made by a human in the moment, though UK law (the Automated and Electric Vehicles Act 2018) assigns initial liability to the insurer.

(b) **L1** Basic identification of the dilemma (e.g. 'the car has to choose who to hurt') with little explanation. **1-2**

(b) **L2** Clear explanation of the ethical challenge using relevant ideas (e.g. utilitarian vs rule-based approaches, differing priorities between individuals/cultures) with some attempt at evaluation. **3-5**

(b) **L3** Sustained, well-reasoned evaluation that considers multiple ethical perspectives and cultural variation, and reaches a justified conclusion about whether universally acceptable rules are achievable. **6-7**

(b) Indicative content:

- This is a variant of the 'trolley problem': there is no action-free option, so the software must be pre-programmed with a rule for an unavoidable harm scenario.
- A utilitarian approach (minimise total harm/number of injuries) may conflict with a rule-based approach (e.g. never deliberately steer towards a person) or with protecting the paying customer (the passenger) above all else.
- Research such as the MIT 'Moral Machine' study has shown that people in different countries and cultures prioritise these dilemmas differently (e.g. some cultures prioritise the young over the old, or pedestrians over passengers, more strongly than others), suggesting a single universally 'moral' rule may not exist.
- Manufacturers face a commercial tension: customers may be less willing to buy a car programmed to sacrifice its own passenger in some scenarios.
- Possible mitigations: transparency about how decisions are made, independent regulation/certification of decision rules, and legal frameworks assigning liability rather than expecting a perfect moral answer.
- A well-reasoned conclusion should recognise that full universal agreement is unlikely given cultural variation, so transparency, regulation and legal accountability may matter more than finding one 'correct' ethical rule.

(b) Answer: N/A - levels-marked extended response.

Question 9

(a) (i) Section 1: unauthorised access to computer material applies **B1**

(a) (i) Valid justification, e.g. he accessed the system without the hospital's consent, regardless of his benign intent, which is sufficient for the Section 1 offence **B1**

(a) (ii) Recognises that publishing the exploit code is not itself an act of unauthorised access, so it does not directly commit the Section 1 or Section 3 offence **B1**

(a) (ii) Valid nuance, e.g. this could potentially fall under Section 3A (making, supplying or obtaining articles for use in a computer misuse offence) if the code is judged likely to be used for such offences, though this is a more complex legal question than (i) **B1**

(a) Answer: (i) Section 1 offence applies to the unauthorised access. (ii) Publishing alone is not a direct access/modification offence, but could potentially engage Section 3A depending on intent and likely use.

(b) Data Protection Act 2018 / UK GDPR **B1**

(b) Explains the requirement to report the breach to the Information Commissioner's Office (ICO) without undue delay, and where feasible within 72 hours **B1**

(b) Explains the requirement to notify the affected patients directly if the breach is likely to result in a high risk to their rights and freedoms **B1**

(b) Explains a possible consequence for the trust, e.g. an ICO fine, reputational damage, a requirement to improve security measures **B1**

(b) Answer: Data Protection Act 2018/UK GDPR requires the trust to report the breach to the ICO within 72 hours where feasible, notify affected patients if the risk is high, and it may face a fine or enforcement action.

(c) **L1** Basic explanation of responsible disclosure or of a legal issue, with limited reference to the scenario and little evaluation. **1-3**

(c) **L2** Clear explanation of responsible disclosure principles and of the limitations of current legislation, with reference to the scenario, and some evaluation, though it may be one-sided. **4-6**

(c) **L3** Sustained, well-structured evaluation that draws directly on the scenario to weigh the interests of researchers, organisations and the public, considers the adequacy of current law, and reaches a well-justified overall conclusion. **7-9**

(c) Indicative content:

- Responsible disclosure norms: report privately first, allow a reasonable fixed period (commonly around 90 days in industry practice) for the organisation to patch the flaw, only publish full technical details afterwards, and ideally withhold or delay publication of working exploit code even then.
- In this scenario, Ryan followed part of the process (private report first) but the hospital trust failed to respond, and Ryan then published full working exploit code rather than a limited disclosure or an extended private escalation, which arguably went beyond responsible practice and directly enabled the criminal attack.
- The Computer Misuse Act 1990 does not provide an explicit statutory defence or 'safe harbour' for good-faith security research; the Section 1 offence can technically apply even where access was for a benign purpose, unlike some other jurisdictions that provide specific protections for authorised or good-faith testing.
- This creates a chilling effect: legitimate researchers may be deterred from testing real systems for fear of prosecution, meaning vulnerabilities may go undiscovered or unreported, reducing overall public benefit.
- Counter-argument: without some deterrent, any unauthorised access could be excused as 'research', which would undermine legitimate prosecution of malicious actors, so the law cannot simply exempt all such access.
- Possible reforms discussed by security professionals include an explicit public interest defence for authorised/ethical security research, wider adoption of formal bug bounty and vulnerability disclosure programmes by organisations, and clearer statutory response-time obligations on organisations receiving vulnerability reports.
- A well-reasoned conclusion should recognise that the harm in this case arose from failures on both sides (the hospital's lack of response and the researcher's decision to publish working exploit code), and that legal reform alongside better organisational processes, rather than either the criminal law or individual ethics alone, is likely needed to properly balance these interests.

(c) Answer: N/A - levels-marked extended response.