NAME DATE STARTED TARGET END DATE

GCE AS LEVEL — COMPUTER SCIENCE UNIT 1 QUESTION PACK

2500U10-1 · 2015 spec Unit 1 Topic 9 · AS unit, first sat 2017, 100 marks, 2h paper

REVISE.wales

COMPUTER SCIENCE — UNIT 1 · Security, Ethics & Use of Computers

Topic 1.8 — Threats to computer systems, contingency planning, Data Protection Act and societal impact

Malicious and accidental damage to data, file-security measures, contingency planning and disaster recovery, the impact of the Data Protection Act on organisations, and the wider effects of computer systems (e.g. expert systems) on employment and society.

2015 specification · current

Estimated time for entire question pack: ~1 h 6 min

Derived from the Unit 1 pace of ~1.2 min/mark, padded for written-prose answers (44 marks over 7 questions).

*You are advised to **not** attempt to complete all of this in one sitting.*

ABOUT THIS QUESTION PACK

This is a **comprehensive topic question pack**, not a single mock paper. It contains every question from the WJEC AS Unit 1 papers (Summer 2017 – Summer 2024, COVID gap) that maps onto Topic 1.8 of the 2015 specification.

Questions are ordered by source paper date.

INSTRUCTIONS

Use black ink or black ball-point pen. Show all working. A calculator is allowed where useful.

For Examiner's use only

Q	Source	Max	Mark
1	S17 Q5	6	
2	S17 Q13	5	
3	S18 Q3	8	
4	S19 Q9	6	

Q	Source	Max	Mark
5	S22 Q12	4	
6	S22 Q13	11	
7	S24 Q8	4	
Total		**44**	

Security, Ethics & Use of Computers — what the spec asks

WJEC GCE AS Computer Science (from 2015) · Unit 1: Fundamentals of Computer Science · Topic 1.8.

Threats to data

- Malicious: viruses, worms, ransomware, phishing, hacking, denial of service.
- Accidental: hardware failure, power loss, user error, fire / flood.
- Insider threats: disgruntled employees, careless data handling.
- Social engineering exploits humans, not technology.

Contingency planning

- Regular backups (3-2-1 rule: 3 copies, 2 media, 1 off-site).
- Disaster-recovery plan: roles, procedures, recovery time objectives.
- Hot / warm / cold standby sites; mirrored servers.
- Test restores periodically — backups you can't restore are worthless.

File security

- Access control: read / write / execute permissions per user / group.
- Encryption at rest and in transit.
- Audit logs of who accessed what and when.
- Anti-virus, firewall, version control, secure deletion of obsolete files.

Data Protection Act / GDPR

- Personal data must be processed lawfully, fairly, transparently.
- Collected for specified, explicit purposes; minimised; accurate; kept up to date.
- Retained only as long as necessary; secured against unauthorised access.
- Subject rights: access, rectification, erasure, portability, object.

Computer Misuse Act

- Unauthorised access to computer material (level 1).
- Unauthorised access with intent to commit further offence (level 2).
- Unauthorised modification of computer material (level 3).
- Making, supplying or obtaining tools to commit these offences.

Societal impact

- Employment: automation displaces routine jobs; creates technical roles.
- Expert systems aid decisions in medicine, law, finance — but raise accountability questions.
- Privacy concerns: tracking, profiling, data brokers.
- Digital divide: access to technology shapes opportunity.

Crib sheet »

Security, Ethics & Use of Computers in one page

Quick-reference notes — revisit before each question.

Malware types

Virus: attaches to file, spreads when run.
Worm: self-propagating across network.
Trojan: hides in legitimate-looking app.
Ransomware: encrypts data, demands payment.

Phishing

Fake email / SMS / call impersonating a trusted entity.
Lures user to surrender credentials.
Mitigate: SPF/DKIM/DMARC, user training, MFA.

Backup strategy

3-2-1: three copies, two media, one off-site.
Test restores periodically.
Versioning protects against silent corruption and ransomware.

DPA principles

Lawful, fair, transparent.
Purpose-limited, minimised, accurate, time-limited.
Confidential & integrity-protected.
Accountable.

Subject rights

Access, rectification, erasure, restriction, portability, objection.
Must respond within statutory time limit.

Computer Misuse Act

1990 in UK.
1: unauthorised access.
2: access with intent to commit further offence.
3: unauthorised modification / impairment.
3A: making / supplying tools.

Examiner only

5. Describe potential threats to computer systems and how contingency planning can help recover from disasters. [6]

Examiner only

13. Explain how the Data Protection Act impacts on an organisation that stores data on a computer system. [5]

Examiner only

3. *(a)* Describe the dangers that can arise from the use of computers to store personal data. [4]

(b) Describe processes that protect the security and integrity of data. [4]

Examiner only

9. Describe methods used in file security to prevent accidental data loss from computer systems. [6]

Examiner only

12. Describe the difference between malicious and accidental damage to data and identify **one** situation where each could occur. [4]

Examiner only

13. Explain the purpose of expert systems and describe the possible effects of these systems on the nature of employment in wider society.

Discuss their general benefits and drawbacks. [11]

END OF PAPER

Examiner only

8. Describe computer-based processes that protect the security of data. [4]

END OF QUESTION PACK

7 questions · 44 marks · ~1 h 6 min
Source: WJEC AS Computer Science Unit 1 (2500U10-1), Summer 2017–2024, COVID gap
Curated for WJEC Computer Science 2015 spec AS Unit 1 — Topic 9 (1.8)