ComputerScience4U.com

AQA

GCSE
Computer Science

8520/2-Paper 2 Written Assessment
Mark scheme

June 2018

Version/Stage: 1.0 Final

Mark schemes are prepared by the Lead Assessment Writer and considered, together with the relevant questions, by a panel of subject teachers. This mark scheme includes any amendments made at the standardisation events which all associates participate in and is the scheme which was used by them in this examination. The standardisation process ensures that the mark scheme covers the students' responses to questions and that every associate understands and applies it in the same correct way. As preparation for standardisation each associate analyses a number of students' scripts. Alternative answers not already covered by the mark scheme are discussed and legislated for. If, after the standardisation process, associates encounter unusual answers which have not been raised they are required to refer these to the Lead Assessment Writer.

It must be stressed that a mark scheme is a working document, in many cases further developed and expanded on the basis of students' reactions to a particular paper. Assumptions about future mark schemes on the basis of one year's document should be avoided; whilst the guiding principles of assessment remain constant, details will change, depending on the content of a particular examination paper.

Further copies of this mark scheme are available from aqa.org.uk

The following annotation is used in the mark scheme:

; - means a single mark

// - means alternative response

/ - means an alternative word or sub-phrase

A - means acceptable creditworthy answer. Also used to denote a valid answer that goes beyond the expectations of the GCSE syllabus.

R - means reject answer as not creditworthy

NE - means not enough

I - means ignore

DPT - in some questions a specific error made by a candidate, if repeated, could result in the candidate failing to gain more than one mark. The DPT label indicates that this mistake should only result in a candidate losing one mark on the first occasion that the error is made. Provided that the answer remains understandable, subsequent marks should be awarded as if the error was not being repeated.

Copyright © 2018 AQA and its licensors. All rights reserved.
AQA retains the copyright on all its publications. However, registered schools/colleges for AQA are permitted to copy material from this booklet for their own internal use, with the following important exception: AQA cannot give permission to schools/colleges to photocopy any material that is acknowledged to a third party even for internal use within the centre.

Level of response marking instructions

Level of response mark schemes are broken down into levels, each of which has a descriptor. The descriptor for the level shows the average performance for the level. There are marks in each level.

Before you apply the mark scheme to a student's answer read through the answer and annotate it (as instructed) to show the qualities that are being looked for. You can then apply the mark scheme.

Step 1 Determine a level

Start at the lowest level of the mark scheme and use it as a ladder to see whether the answer meets the descriptor for that level. The descriptor for the level indicates the different qualities that might be seen in the student's answer for that level. If it meets the lowest level then go to the next one and decide if it meets this level, and so on, until you have a match between the level descriptor and the answer. With practice and familiarity you will find that for better answers you will be able to quickly skip through the lower levels of the mark scheme.

When assigning a level you should look at the overall quality of the answer and not look to pick holes in small and specific parts of the answer where the student has not performed quite as well as the rest. If the answer covers different aspects of different levels of the mark scheme you should use a best fit approach for defining the level and then use the variability of the response to help decide the mark within the level, ie if the response is predominantly level 3 with a small amount of level 4 material it would be placed in level 3 but be awarded a mark near the top of the level because of the level 4 content.

Step 2 Determine a mark

Once you have assigned a level you need to decide on the mark. The descriptors on how to allocate marks can help with this. The exemplar materials used during standardisation will help. There will be an answer in the standardising materials which will correspond with each level of the mark scheme. This answer will have been awarded a mark by the Lead Examiner. You can compare the student's answer with the example to determine if it is the same standard, better or worse than the example. You can then use this to allocate a mark for the answer based on the Lead Examiner's mark on the example.

You may well need to read back through the answer as you apply the mark scheme to clarify points and assure yourself that the level and the mark are appropriate.

Indicative content in the mark scheme is provided as a guide for examiners. It is not intended to be exhaustive and you must credit other valid points. Students do not have to cover all of the points mentioned in the Indicative content to reach the highest level of the mark scheme.

An answer which contains nothing of relevance to the question must be awarded no marks.

<table>
<tr><th>Qu</th><th>Part</th><th>Marking guidance</th><th>Total marks</th></tr>
<tr><td>01</td><td>1</td><td>Mark is for AO2 (apply)

156;</td><td>1</td></tr>
<tr><td>01</td><td>2</td><td>2 marks for AO2 (apply)

9C;;

If the answer given is not 9C then award as follows:

1001 converted to 9;
1100 converted to C;

Max 1 mark if final answer is not correct.</td><td>2</td></tr>
<tr><td>02</td><td></td><td>2 marks for AO2 (apply)

10101010;;

One mark if the right hand side 4 bits are correct (1010)
One mark if the left hand side 4 bits are correct (1010)</td><td>2</td></tr>
<tr><td>03</td><td></td><td>3 marks for AO1 (understanding)

<table><tr><th>Capacity</th><th>Order (1-4)</th></tr><tr><td>0.5 Terabytes</td><td>4</td></tr><tr><td>3500 Kilobytes</td><td>1</td></tr><tr><td>2.5 Gigabytes</td><td>2</td></tr><tr><td>6250 Megabytes</td><td>3</td></tr></table>
3 marks for all four correct
2 marks for two correct
1 mark for one correct

In this instance, alternatively formed responses were credited as appropriate.</td><td>3</td></tr>
<tr><td>04</td><td>1</td><td>Mark is for AO2 (apply)

01100110;</td><td>1</td></tr>
</table>

04	2	**2 marks for AO2 (apply)** 256;; If the answer given is not 256 then award a **maximum of one** working out mark for any of the following: • 4 bits per pixel/colour; • 8 * 8 = 64; • Multiplying 64 by any integer; **R.** 4 bits on its own	2

05		**2 marks for AO1 (recall)** **1 mark: C:** ROM is commonly used to store start-up instructions **1 mark: D:** ROM is non-volatile **If more than two lozenges shaded then marks are not awarded.**	2

06		**4 marks for AO1 (understanding)** 1 mark for each correct point that explains how a Hard Disk Drive operates, up to a maximum of 4 marks. **<u>Examples Include</u>**: • A HDD can contain multiple platters (disks); • A disk/disks that move/spin • Each platter is divided into sectors; • The disks are spun at a very high speed (approximately 7,200 rpm to 10,000 + rpm); • Read\write heads (move across the disk to) read and write data; • There is one read\write head for each side of a platter ie two heads per platter; • Data is written to\read from the disk by magnetising\polarising\sensing microscopic regions on the disk; • Data is organised in concentric rings called tracks; • There is a small circuit board on the drive that controls the reading and writing of data; • Data is transferred from and to the disk via a cable/electrical current being passed; • The intersection of sectors and tracks are called blocks; • Data is read 1 block at a time; **NE** Storing binary, or 1s and 0s without reference to magnetising	4

07	1	**Mark is for AO1 (recall)** AND (gate);	1

07	2	**Mark is for AO1 (recall)** OR (gate) ;	1

07	3	**Mark is for AO1 (recall)** 1 mark for any of the following: • A NOT gate is used to flip/invert/switch an input • The output will be the opposite of the input • 0s become 1 **and** 1's become 0s;	1

07	4	**3 marks for AO2 (apply)** INPUTS: A, B, C; A AND B: D; C OR D: E; D OR E: F | A	B	C	D	E	F
---	---	---	---	---	---
0	0	0	0	0	0
0	0	1	0	1	1
0	1	0	0	0	0
0	1	1	0	1	1
1	0	0	**0**	**0**	**0**
1	0	1	0	1	1
1	1	0	1	**1**	**1**
1	1	1	**1**	**1**	**1**	 1 mark for column D correct 1 mark for column E correct 1 mark for column F correct **A.** Follow through for column F based on incorrect but complete columns D or E	3

<table>
<tr>
<td>08</td>
<td>1</td>
<td>3 marks for AO1 (recall), 3 marks for AO1 (understanding)

Max 3 marks for stating the components.
Max 1 description mark for each component stated.

<table>
<tr><td>Control Unit;</td><td>Decodes instruction;
Controls the fetching and writing of data;</td></tr>
<tr><td>Arithmetic Logic Unit/ ALU;</td><td>Executes mathematical instructions;
Executes logical instructions;
Compares values held in registers;</td></tr>
<tr><td>Clock;</td><td>Controls the number of instructions carried out each second;
Allows the CPU to synchronise operations;

R. allows the computer to display the time</td></tr>
<tr><td>Bus;</td><td>Used to transfer data / instructions from one component of the CPU to another;

A. Variations such as Control bus, Address bus, Data bus</td></tr>
<tr><td>(L1) Cache;</td><td>Very fast memory;
Memory close/on CPU;
Stores frequently used instructions/data;</td></tr>
<tr><td>Register;</td><td>Special purpose (small) memory location (on CPU);
Used for specific purpose in Fetch-Execute Cycle;</td></tr>
</table>

R. RAM/ROM/IAS.</td>
<td>6</td>
</tr>
</table>

<table>
<tr>
<td>08</td>
<td>2</td>
<td>Mark is for AO1 (recall)

decode;

I. Minor spelling errors or hyphenated word
I. Case</td>
<td>1</td>
</tr>
</table>

09		**3 marks for AO1 (understanding)** 1 mark for each valid reason given up to a maximum of 3 marks. **<u>Examples include</u>**: • To allow sharing of files; • To backup files from a PC; • To allow remote access of files/access from anywhere; • To allow access from any computer/device (with internet access); • To give access to a larger amount of storage capacity; • To allow concurrent access\collaboration; • Can purchase a cheaper (lower spec) computer; • Cloud storage is automatically backed up by the host; • May be more fault tolerant/resilient than local storage; **R**. Relative cost, unless statement is qualified.	3

10	1	**2 marks for AO1 (understanding)** – maximum of two marks. System software manages the computer hardware\application software; application software is for end-user tasks; **A.** answers that give two separate differences even if just mentioning application software or system software as it would imply the opposite is true for the opposing type. **R.** References to pre-installed/downloaded software.	2

10	2	**2 marks for AO1 (recall), 2 marks for AO1 (understanding)** AO1 Understanding – 1 mark each for the function (to a maximum of 2 marks), 1 mark for descriptions (to a maximum of 2 marks). Memory management • Manage the computer's memory; • It can control which parts of memory are being used by which process; Processor management • Manage the computer's processor(s)CPU; • Schedules which processes are to be executed; Input/output management • Manages input/output devices; • Interacts with/manages/handles the (automatic) installation of device drivers; • Handles peripheral device interrupts; • the computer can communicate with the outside world; • Control network communication; • Allow devices to send and receive data; Managing storage • Manage secondary storage devices; • Loading data and programs into the computer's memory; • Storage space management (disk quotas); • To ensure that storage space is allocated fairly and efficiently to specific tasks\users; Managing security • User authentication; • To make sure that users must prove who they are to access the system; • Protect against malware; • Block access to specific vulnerable operations or system areas. For example, software can only be installed with admin access; Managing applications • Control access to applications; • Prevent users or processes using unauthorised programs // allow users or processes to use authorised programs; • Control application access; • Prevent/allow an application access to data (or devices); **A.** User interface (maximum of 1 mark)	4

10	3	**2 marks for AO1 (understanding)** AO1 understanding – **1 mark** for each identified error **maximum of 2** marks. Hardware is a physical device or component // (and therefore) it cannot be downloaded or installed from a disk; Software are programs (that get installed onto a computer); **A.** the student has said "the student has explained software and hardware back to front\the wrong way around" – **max 1 mark** if this is the only response.	2

11	1	**4 marks for AO1 (understanding)** **1 mark** for each explanation point. **Example answers** • A WAN is a Wide Area Network that links more than one remote geographical site/location to another; • A LAN is a Local Area Network that links together devices that are within one site\location; • The speed of data transmission across a LAN is likely to be higher than across a WAN; • WANs are typically public networks (and so data encryption is likely to be used); • LANs (may not need data encryption) as they are typically private; • LANs typically carry less traffic than WANs; • This is because the number of users on a LAN can be controlled by the administrator whereas public WANs could have an unlimited number of users; • LAN Connections are generally more reliable as they are under the control and maintenance of the network administrators; • On a WAN it is possible that heavy traffic, peak usage times, viruses, weather or physical damage could affect the connection reliability; • WANs are typically under shared ownership; • LANs are typically owned by a single person or organisation; • LANs use different protocol suites (accept protocols) to WANs; **R**. Simple expansion of acronyms. **R**. Any reference to cost comparisons. **R**. Reference to cable types. **R**. WAN is a collection of LANs/LANs joined together (if only a simple statement).	4

11	2	**Mark is for AO1 (understand)** **Max 1 mark** for any of the following: • HTTPS is secure/encrypted; • Data transmitted using HTTP could be easily read if intercepted; • Data transmitted using HTTPS can only be seen/read/understood by the (intended) recipient;	1

11	3	**2 marks for AO1 (recall)** **1 mark** for each correct answer. Accept any of: • Transport (layer); • Data Link (layer); • Link (layer); • Network Interface/access (layer) **R.** Any name that is not correct. **I.** the order that the answers are written in	2

11	4	**2 marks for AO1 (understanding)** Max 2 marks: • packages/unpackages data (for/after transmission); • adds address(es) (for transmission); • routes the packets (across the network); • provides error checking; **R.** It provides access to the Internet	2

11	5	**2 marks for AO1 (understanding)** **1 mark** for each of the following points to a maximum of 2 marks. • Each device connected to the network has a (unique) reference ID/physical address (called the MAC Address); • There is a list of allowed/denied addresses; • The network device/router looks at the address of the device trying to connect (and blocks/allows appropriately);	2

12		**3 marks for AO1 (understanding)** 1 mark each for describing the social engineering technique. **Blagging (pretexting)** This is where a victim is tricked/persuaded (by a fraudster) to give their details or payment information (for a fraudulent reason/purpose); **Phishing** Is where the victim receives and responds to a communication that appears to be from a valid or known source (but is in fact fraudulent. It allows the fraudster to capture private information before the victim realises); **Shouldering (or shoulder surfing)** This is where someone watches and records\remembers a victim entering their pin or security information such as passwords. (They can then use this information to gain access to a system);	3

13	1	**3 marks for AO2 (apply)** **Character** / **Binary Code** G / 10; S / 110; H / 111;	3

<table>
<tr>
<td>13</td>
<td>2</td>
<td>
4 marks for AO2 (apply)

66 (bits);;;;

A. other answers if they are correct based on incorrect answer provided for 13.1 but only if the working has been shown.

If the answer given is not correct based on their answer to Q 13.1, a maximum of 3 working out marks should be awarded as follows:

<u>Huffman Tree Calculation</u>

5*1 + 4*2 + 2*3 + 2*3 // 25 (bits) // (length of) 0010111111101011000011010 (1 mark);

A. a calculation that results in an answer that is not 25 bits as long as the maths is all correct (ie incorrect frequencies or bit counts have been used)

<u>ASCII Calculation</u>
13 characters * 7 bits // 91 (bits) (1 mark);

<u>Calculate Saving</u>
Subtracting ASCII bit total minus Huffman bit total (1 mark);

Example 1 Incorrect Huffman Tree Calculation

This table below shows incorrect codes given by a student.

<table>
<tr><th>Character</th><th>Binary Code</th></tr>
<tr><td>A</td><td>0</td></tr>
<tr><td>G</td><td>010</td></tr>
<tr><td>S</td><td>0110</td></tr>
<tr><td>H</td><td>0111</td></tr>
</table>

5 (Letter A freq) * given length +
4 (Letter G freq) * given length +
2 (Letter H freq) * given length +
2 (Letter S freq) * given length

5 * 1 +
4 * 3 +
2 * 4 +
2 * 4 = 33 bits

If performed correctly based on binary code lengths given in answer 13.1 this would be given 1 mark.

Student gets ASCII length correct (this would be given 1 mark)

If the student then used this value to calculate the saving 91 bits – 33 bits = 58 then this would be given 1 mark.

A total of 3 marks would be given.
</td>
<td>4</td>
</tr>
</table>

Example 2 Incorrect Huffman Tree Calculation

This table below shows **incorrect** codes given by a student.

Character	Binary Code
A	0
G	010
S	0110
H	0111

5 * 4 + (incorrect length)
4 * 4 + (incorrect length)
2 * 4 +
2 * 4 = 52 bits

Calculation is correct but lengths are wrong based on binary code lengths given in answer 13.1 (this would be given zero marks).

Student gets ASCII length correct (this would be given 1 mark)

If the student then used this value to calculate the saving 91 bits – 52 bits = 39 bits then this would be given 1 mark.

A total of 2 marks would be awarded.

14

6 marks for AO2 (apply)

Level	Description	Mark Range
3	**Explanation** of at least **three** issues that are clearly related to an organisation rather than the end user. **or** **Explanation** of **two** issues that are clearly related to an organisation and **described** at least **one** other.	5-6
2	**Explanation** of **two** issues that are clearly related to an organisation rather than the end user. **or** **Explanation** of **one** issue and **description** of **at least one other** issue clearly related to an organisation. **or** **Description** of **three** issues that may not be related to an organisation.	3-4
1	**Explanation** of **one** issue which does clearly relate to an organisation. **or** **Description** of **one** or **two** issues that may not be related to an organisation.	1-2
No creditworthy material		0

6

Guidance:

- Websites – any inappropriate websites ie pornography, drugs, guns, terrorism etc. e.g. is it acceptable for the organisation to allow access to this sort of material when you can't control who is accessing the service?
- Time – limit amount of time, they may not want to provide indefinite access or may want to charge for access after the time limit has expired.
- Preventing file sharing and illegal sharing\use of copyrighted materials.
- Accountability – identification of users and actions on a network by preventing anonymous access.
- Prevention of illegal activities such as terrorism and fraud.
- The responsibility to keep children safe and protected.
- Responsibility to keep users (customers) data safe and secure.
- Spoofing of websites, phishing. Responsibility of organisation to put some kind of protection in place, eg filtering of known fraudulent sites.
- Recording of private messages or details if not encrypted.
- Recording of usernames and passwords that the user may also use to access other systems.
- Responsibility of organisation to secure their systems from possible attack.
- Sales and marketing – providing sales leads to market products.

<table>
<tr><td>15</td><td></td><td>4 marks for AO1 (understanding) and 8 marks for AO2 (apply)
<table>
<tr><th>Level</th><th>Description</th><th>Mark Range</th></tr>
<tr><td>4</td><td>Level 4 High mark range
Subject Criterion Context

A clear understanding shown through the use of at least four relevant examples that discuss the methods a company or individual could use to protect their devices from malware and/or minimise the damage caused by infection.

Examples are well supported by reasoned arguments and the detail given should explain how and why the methods\techniques would be in/effective.</td><td>10-12</td></tr>
<tr><td>3</td><td>Level 3 Higher mid mark range
Subject Criterion Context

A more developed understanding shown through the use of suitable examples that discuss\explain at least three methods a company or individual could use to protect their devices from malware and/or minimise the damage caused by infection.

Examples are supported by explanations of how the methods\techniques would be in/effective.</td><td>7-9</td></tr>
<tr><td>2</td><td>Level 2 Lower mid mark range
Subject Criterion Context

Some understanding shown through the use of suitable examples that describe at least two methods a company or individual could use to protect their devices from malware and/or minimise the damage caused by infection.

Examples are supported by limited descriptions and at least one explanation of how the method\technique would be in/effective.</td><td>4-6</td></tr>
<tr><td>1</td><td>Level 1 Lower mark range
Subject Criterion Context

At the higher end of the mark range there is a simple description about at least one method\technique that could be used by a company or individual to protect their devices from malware and/or minimise the damage caused by infection. The answer may not include an explanation of how the method(s) would work.

Simple statements\example(s) of methods\techniques (for example a bulleted list) supported by no comments is limited to the middle of this range.</td><td>1-3</td></tr>
<tr><td colspan="2">No creditworthy material</td><td>0</td></tr>
</table></td><td></td><td>12</td></tr>
</table>

Method AO1 (Understanding)	Explanation AO2 (apply)
Regularly back up data and test backups.	Back up data so that you can restore data that has been accidentally deleted or destroyed. It is important to test that back-ups work on a regular basis.
Secure the backups.	Make sure that backups are off site so they are not lost under the same circumstances as the main data. Also if the backups are air-gapped then this will prevent a severe malware infection getting access to the backups as there is no physical connection.
Block or remove email attachments or links.	Check links contained in e-mails and do not open attachments included in unexpected e-mails.
Disable pop-ups.	Ensure the pop-up blocker is turned on and any website screening options are also on.
Control software downloads.	Only download software, especially free software, from sites you know and trust. Or prevent software downloads completely.
Ensure software is up to date.	Make sure all software is up to date and patched to prevent any exploitation of known vulnerabilities.
Anti-virus is up to date.	Ensure anti-virus automatically updates so that the latest vulnerabilities are detected and dealt with.
Disable macro scripts.	Prevent macros from running which could cause or run malicious code.
Only allow specified programs to run.	Preventing any unknown programs running should prevent any malicious code before it gets a chance to run.
Manage the use of privileged accounts and access levels to files.	Controlling the access to files should act as an internal firewall\barrier to prevent unauthorised access or execution of programs.
Use virtualized environments\sandboxes.	Operations are carried out in a controlled and temporary working space\environment which can be easily reset without effecting anything outside of the space\environment.
Use network filtering or a firewall.	Prevent\block access into and out of the network using filtering and firewall to stop any malicious communications or transfer of viruses.
Remove the ability to use removable media.	Prevent unknown or unauthorised files to enter or leave the network.
MAC address filtering.	Can prevent access by unauthorised devices.
User training.	To educate staff in dangers of social engineering techniques and other unsafe practices.
Pen testing.	To allow organisation to understand where weaknesses may be, in order to strengthen their system security.

R. Encryption, unless it is discussed in terms of minimising damage