01		**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

02	3	**4 marks for AO1 (understanding)** Maximum of 3 marks if only1 type of testing. **Black box testing:** • the tester does not know how the system operates; • the tester is acting as an external hacker; • requires a lot of investigation and guessing/brute-force to find issues; • may not test all of the system especially if you do not know it's full functionality; • you are trying to discover and exploit the weak spots in the system; **White box testing:** • the operation of the system is known; • the tester is simulating a malicious insider; • can be targeted to test specific vulnerabilities; • you know exactly what you are trying to test; • because you know what you are testing you should be able to test all possible scenarios; **R.** Any direct opposites. Statements such as "Black box has no knowledge of how the system operates. White box has knowledge of how the system operates." would be awarded only one mark.	4

03		**3 marks for AO1 (recall), 3 marks for AO1 (understanding)** 1 mark each for stating, 1 mark each for describing. • Trojan (horse); a program which misleads the user into thinking it is another piece of software which, when run, executes another program; • Spyware; a program which records data such as usernames and passwords on a host system and forwards the information to a third party; • Adware; code embedded or attached to program files which will persistently show adverts (that attempt to generate revenue); • Worm; code which will run autonomously and replicates itself on a host system; • Ransomware; a program that encrypts user's data to make it unreadable until they pay for the key; • Remote Access Tool (RAT); allows access to control and monitor a computer from a remote network location; • Rootkit; malware that has managed to gain 'root' admin privileges; • Bots/Zombies; a program installed on a computer that performs a job for the remote owner of the bot/zombie such as sending spam or sending web requests to perform a DOS or attacking a computer system; • Scareware; malware that tells you something is wrong with your system in an attempt to get you to make a purchase; • Keylogger; a program that monitors/records a user's keystrokes in order to steal passwords/confidential details; **R.** Specific named examples on their own, eg "Wannacry" would receive no marks, "Ransomware such as Wannacry" would receive 1 mark. **R.** References to 'virus' as this is the example in the question.	6

Qu	Part	Marking guidance	Total marks
04	1	**2 marks for AO1 (recall)** • (the processes/practices/technologies/methods designed to) protect networks/computers/programs/data; • from attack/damage/threats/unauthorised access;	2
04	2	**2 marks for AO1 (recall)** • (Malware is a blanket/umbrella term for) computer software/program/code; • with malicious/hostile/intrusive intent;	2

<table>
<tr><th>Qu</th><th>Part</th><th>Marking guidance</th><th>Total marks</th></tr>
<tr><td>04</td><td>3</td><td>8 marks for AO2 (apply)
<table>
<tr><th>Level</th><th>Description</th><th>Mark Range</th></tr>
<tr><td>4</td><td>Responses at this level will contain a thorough explanation of how all of the threats could be exploited by a student. The response makes clear reference to a school network. The response is well structured and coherent.

More than one consequence has been described.</td><td>7–8</td></tr>
<tr><td>3</td><td>Responses at this level will contain a detailed explanation of how most of the threats could be exploited by a student. The response makes clear reference to a school network. The response is well structured and coherent.

At least one consequence has been described.</td><td>5-–6</td></tr>
<tr><td>2</td><td>Responses at the upper end of the level will contain some explanations of how most of the threats could be exploited by a student. The response makes some reference to a school network. The response makes sense when read as a whole.

Responses at the lower end of the level will mostly contain descriptions of how some of the threats could be exploited by a student. The response might make some reference to a school network. The response makes some sense when read as a whole.

In this level students may not have referred to the consequences.</td><td>3–4</td></tr>
<tr><td>1</td><td>Responses at the upper end of the level will contain descriptions of at least one of the threats and/or consequences.

Responses at the lower end of the level will include a few statements related to one or more of the required threats/consequences.</td><td>1–2</td></tr>
<tr><td colspan="2">No creditworthy material</td><td>0</td></tr>
</table></td><td>8</td></tr>
</table>

		Indicative Content The indicative content below is written in a generic manner for the benefit of examiners. Responses should be worded in the context of a school to gain the highest marks. For example reference to pupils using default passwords or them gaining access to staff-only areas through misconfigured access rights. • Weak and default passwords: o students could use brute force methods to crack passwords o weak admin passwords would allow students to gain admin level access o default passwords allow students to gain access without any effort o default passwords published online so everyone knows them. • Misconfigured access rights: o allows students to access areas they are not supposed to o network admins might not know that secure areas had been breached as no-one has 'broken in' o students could reconfigure network o students could create new user accounts to give themselves admin access. • Removable media: o could contain malware that allows students to gain access to network o could be used to steal data o could be used to allow students to take control of certain network processes (eg remote access systems). • Unpatched and/or outdated software: o could allow students to exploit known weakness/flaw o known weaknesses/flaws are published online o once in a student could install malware.	

04	4	**1 mark for AO1 (recall)** **C** The art of manipulating people so they give up confidential information. **R.** if more than one lozenge shaded.	1

Qu	Part	Marking guidance	Total marks
04	5	**4 marks for AO2 (apply)** A **maximum of 4 marks** can be awarded. **One mark** for each point and **one mark** for an expansion. Answers that are too similar to each other must only be credited once. Example responses include: • Train staff/students to be cautious of emails; o that come from unrecognised senders; o that ask you to confirm personal/financial information (over the Internet); o that make urgent requests for personal/financial information; o that are not personalised; o that try to upset you into acting quickly by threatening you with frightening information; • Train staff/students not to click on links/download files/open attachments (in emails); from unknown senders/sources; • Prevent students from being able to download; anything from the internet/email links; • Train staff/students to never enter personal information; in a pop-up screen; • Train staff/students not to copy web addresses (into a browser); from pop-ups; • Protect the school computers with a firewall/spam filters/anti-virus/anti-spyware software; and keep the software updated;	4

Qu	Part	Marking guidance	Total marks
05	1	**2 marks for AO1 (understanding)** Maximum of **two** marks from: • (weak) passwords are easily cracked // a program could be used to try out lots of passwords // users might choose passwords which are not strong enough // (weak) passwords can be easily guessed; • usernames/passwords may have appeared in data leak; • (if users write down/store their passwords) these can be stolen; • susceptible to shouldering; • it is difficult to verify the actual identity of the person logging in (eg compared to fingerprint/Touch/facial recognition/Face ID, multi-factor authentication);	2

Qu	Part	Marking guidance	Total marks
06	1	**2 marks for AO1 (recall)** Maximum **one** mark from: • the process of attempting to gain access to resources/a computer system; • the practice of testing a computer system/network/web application // to test the effectiveness of security measures; Maximum **one** mark from: • without knowledge of usernames/passwords/other normal means of access; • to find vulnerabilities/weaknesses (that an attacker could exploit);	2

Qu	Part	Marking guidance	Total marks
06	2	**2 marks for AO1 (recall)** to simulate (an attack from) a (malicious) insider; who has knowledge of / basic credentials for the target system;	2

Qu	Part	Marking guidance	Total marks
07	1	**2 marks for AO1 (recall)** (The processes / practices / technologies designed) to protect networks / computers / programs / data; from attack / damage / unauthorised access;	2

Qu	Part	Marking guidance	Total marks
07	2	**Mark is for AO1 (recall)** (Computer) Virus; Trojan; Spyware; **Maximum of 1 mark.** **A.** other types of malware not specified in specification, such as: Worms Adware Ransomware Rootkits **R.** specific malware names such as Stuxnet, WannaCry unless used as an example to support a correct answer	1

<table>
<tr><th>Qu</th><th>Part</th><th>Marking guidance</th><th>Total marks</th></tr>
<tr><td>07</td><td>3</td><td>
9 marks for AO2 (apply)
<table>
<tr><th>Level</th><th>Description</th><th>Mark Range</th></tr>
<tr><td>3</td><td>Answer tackles all of the threats listed in the question and demonstrates a clear understanding of both how the threats could be exploited and how AQAware could protect themselves against the threats. Explanations are clear and detailed.

A range of relevant examples are covered and these are clearly focused on how the company can protect its systems.</td><td>7–9</td></tr>
<tr><td>2</td><td>Answer tackles most or all of the threats listed in the question and demonstrates some understanding of how the threats could be exploited and how AQAware could protect itself against the threats. Explanations are generally clear but sometimes lack detail.

Some relevant examples are mentioned and these are generally focused on how the company can protect its systems but may sometimes stray into referring to individual users.</td><td>4–6</td></tr>
<tr><td>1</td><td>Answer tackles one or more of the threats listed in the question and demonstrates a limited understanding of how the threats could be exploited and/or how AQAware could protect itself against the threats. Explanations may not always be clear.

Examples may be provided but these may not always be focused on how the company can protect its systems and may stray into general points about computer security.</td><td>1–3</td></tr>
<tr><td>0</td><td>No creditworthy material.</td><td>0</td></tr>
</table>
<u>Indicative Content</u>

How the threat could be exploited:

Weak and default passwords
• hackers could use brute force methods to crack passwords
• weak admin passwords would allow hackers to gain admin level access
• default passwords allow hackers to gain access without any effort
• default / stolen passwords published online so that everyone can find them.

Misconfigured access rights
• allows staff to access areas they are not supposed to
• network admins might not know that secure areas had been breached as no-one has ‘broken in’
• staff could reconfigure network
• staff could create new user accounts to give themselves admin access.
</td><td>9</td></tr>
</table>

Unpatched or outdated software

- could allow staff or hackers to exploit known weakness / flaw
- known weaknesses / flaws are published online
- once in a hacker could install malware.

How AQAware could protect themselves:

Weak and default passwords

- enforce a strong password policy, including admin accounts on all devices, across the company with passwords that are regularly changed // force users to change their passwords regularly to strong ones.
- ensure default passwords are changed on all devices
- implement biometric measures such as fingerprint / facial / retinal scans for user authentication.

Misconfigured access rights

- careful application of suitable access rights across the network reducing the level of access level of any one individual
- make sure users only have access to the data / software they need
- give read-only access instead of full access where possible
- ensure that only relevant accounts have access to change DNS files.

Unpatched or outdated software

- software patches and updates are applied regularly (automatically) to keep the systems up to date, ensuring any recently discovered bugs or security issues are patched.

A. Any sensible threat and relevant protection method

Qu	Part	Marking guidance	Total marks
08		**3 marks for AO1 (understanding)** 1 mark each for describing the social engineering technique. Blagging This is where a victim is tricked/persuaded by a fraudster to give their details or payment information for a false 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 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

Question	Part	Marking guidance	Total marks
09		**4 marks for AO1 (understanding)** **Note for examiners:** **Maximum of two** marks if only **one** of blagging or phishing described **Maximum of four** marks from: **Both** blagging and phishing: MP1. Attempt to persuade person to divulge private / sensitive information / make payments; MP2. (Potentially) leading to identity / financial theft / data theft / access by unauthorised persons; MP3. Making up a (convincing) story; Blagging: MP4. Targets an individual; Phishing: MP5. Can be done by email / text / social media; MP6. Disguised to look as though from reputable source / organisation / company; MP7. Targets a large group of people (hoping to get some to respond); MP8. Often contains a link to click on, directing you to a fake website;	4

Question	Part	Marking guidance	Total marks
10		**4 marks for AO1 (understanding)** Maximum of **four** marks. **Note for examiners:** Marks are for the **description only**, not the name of the malware. Description must match the named malware to be credited. **Maximum of two** marks for any one form of malware. Virus: MP1. Can spread when executed; MP2. Attached to another program/file; MP3. Executed by clicking on host/infected program; Trojan: MP4. Poses as having a useful purpose / legitimate program (but has a malicious purpose); MP5. The user is tricked into executing the Trojan // when the program is executed the Trojan activates; **R.** downloading in place of executing Spyware: MP6. Gathers information about person/accounts/organisation/(computer) activity without their knowledge; MP7. Sends information back to originator;	4