



CRESCENT GIRLS' SCHOOL
SECONDARY FOUR
PRELIMINARY EXAMINATION 2021

COMBINED HUMANITIES

2272/1
2273/1
2274/1

Social Studies

24 August 2021

Marking Scheme

1	Study Source A. Why did the university IT support department publish this on their web page? Explain your answer using details of the source.	[5]
L1	Describes the source / repeats provenance	[1]
L2	Identifies sub-message, unsupported <i>Award 2m for identifying any sub-message, unsupported</i>	[2]
L3	Sub-message, supported OR Main message, unsupported <i>Award 3m for sub-message, supported</i> <i>Award 3m for main message, unsupported</i> E.g. This poster was published to show the dangers of not securing their home networks.	[3]
L4	Explains Message, supported <i>Award 4m for explaining Message, supported</i> Message only: E.g. This poster was published to warn the public not to be complacent about securing their home network. The cartoon shows a character saying “It is if that someone uses your account for malicious activities, such as sending emails...” followed up by a panel where police are approaching the other character for investigations of an email bomb threat. This shows that by not securing her network, the character has allowed someone to tap onto her wireless network illegally to send an e-mail threat that had been traced back to her location, even though she was not the actual culprit. The cartoonist is suggesting that this can happen to the public too, if they are not careful.	[4]
L5	Infers Purpose, based on Message, fully explained, supported <i>Award 5m for explanation of purpose, supported</i> Message and purpose: E.g. The poster was published to remind the university students and staff of the consequences of not securing their home networks, so that they take the necessary precautions and protect their home networks with a password and prevent illegal use. The cartoon shows a character saying “It is if that someone uses your account for malicious activities, such as sending emails...” followed up by a panel where police are approaching the other character for investigations of an email bomb threat. This shows	[5]

	that by being complacent and not securing her network , the character has allowed someone to tap onto her wireless network illegally to send an e-mail threat that had been traced back to her location, even though she was not the actual culprit. The cartoonist is suggesting that this can happen to the public too, if they are not careful.	
--	---	--

2	Study Sources B and C. How similar are the two sources? Explain your answer.	[7]
L1	Identifies agreement/disagreement in provenance/topic/source type	[1]
L2	Identifies agreement/disagreement in content, unsupported False Matching <i>Award 2m for identifying similarity AND/OR difference, unsupported</i> False matching: Source B shows that SMEs are victims of cybercrime, while Source C does not.	[2]
L3	Similar OR different in content, supported <i>Award 3m for explaining 1 point of similarity OR difference, supported but no common criteria</i> <i>Award 4m for explaining 1 point of similarity OR difference, supported with clear common criteria</i>	[3-4]
L4	Similar AND different in content, supported <i>Award 5m for similarity and difference, supported but no common criteria</i> <i>Award 6m for similarity and difference, supported with clear common criteria</i> Similarity: The sources are similar in saying that more can be done to ensure that Singaporeans/ individuals are aware of and vigilant against cybercriminal activity. Source B says that “Almost half also recognise that there should be clearer communication from the management to the employees about the importance of cyber security”. This shows that there are many incidents of cybersecurity lapses that could have been prevented through proper education of employees by the respective SMEs. Source C says that “There are still many ways to improve and ensure that Singaporeans are aware of such cyber-scams” which shows that more can be done to ensure	[5-6]

	<p>that Singaporeans are better educated and have a better awareness of cybercrime.</p> <p>Difference: The sources are different in whether Singaporeans are ready to protect themselves against cybercrime. Source B says that “Just over half of the cyber incidents that SMEs suffered in the past 12 months were caused by employees – either through administrative errors or through the loss or theft of a company device such as a laptop or USB drive”. This shows that many individuals are still not careful enough and this leads to cyber incidents, showing that Singapore is still not necessarily ready to protect itself against cybercrime. On the other hand, Source C states, “43 percent of Singapore respondents chose not to interact with scammers – the fourth highest in the world”. This shows that Singaporean consumers are amongst the most careful in the world about online scams, showing that Singapore is ready to protect itself against cyber crime.</p>	
L5	<p>Different in Purpose, explained <i>Award 6m for Purpose, supported only.</i> <i>Award 7m for L3 + Purpose</i></p> <p>The sources are different in purpose. Source B was published to share the trends in the readiness of SMEs for cybersecurity, and convince SMEs of the importance of being more vigilant, so that they would be more prepared for cybercrime, and perhaps even consider using Chubb’s insurance services in the face of such uncertainty. This is seen in “This is worrying, as complacency invites malicious attacks, future breaches and inadequate incident response.”, which shows that Chubb’s is trying to convey the importance of taking cybersecurity seriously to its audience, the SME leaders reading the report. On the other hand, Source C was published to share the trends in the readiness of Singaporean consumers and remind them to continue being prepared and alert to online scams. This is seen in “Even so, there is also a small percentage of young adults and males in Singapore that have fallen prey to such technical support scams. There are still many ways to improve and ensure that Singaporeans are aware of such cyber-scams.” This shows that despite Singaporeans being amongst the most vigilant in the world, some are still falling prey to these scams, and more can be done to minimise cyber-crime.</p> <p>(accept similarity in purpose if students interpret audience of Source B to be Singaporeans, rather than Singaporean SMEs, with the intended impact of convincing its audience to be more</p>	[6-7]

	vigilant/careful) – However, students cannot choose both as it would be contradictory.	
--	--	--

3	<p>Study Sources D and E.</p> <p>How far does Source E prove that the views expressed in Source D are justified?</p> <p>Explain your answer.</p>	[7]
L1	Explain provenance, no use of source content, description of source, general comments	[1]
L2	Prove/Does not prove justified based on similarity/difference in content, unsupported	[2]
L3	<p>Proves OR does not prove justified, based on agreement/disagreement in content, supported</p> <p>OR</p> <p>Proves OR does not prove justified, based on CR of E alone without comparison between D and E (CR Premise must be common between both sources)</p> <p><i>Award 4 marks for well-explained answers</i></p>	[3-4]
L4	<p>Proves AND Does not prove justified, based on agreement/disagreement in content, supported</p> <p><i>Award 5 marks for well-explained and supported answers on both sides</i></p> <p>Source E proves that the views expressed in Source D are justified as they both agree that there is a need for Singaporeans to be better educated in cybersecurity. Source D states “I think the government needs to increase their efforts to educate the people on the importance of cyber-security in today’s time.” This shows that Source D believes that governments need to ensure that the citizens are sufficiently informed about the threat posed by cybercrime. This is supported by Source E, which says “To better protect the cyber system, Singaporeans need to be educated sufficiently regarding the threats of cyber-attacks”, which shows that Source E believes that governments need to teach Singaporeans regarding the consequences of cyber-threats. Thus, since Source E supports Source D, it proves that the view on the need to educate Singaporeans is justified.</p>	[4-5]

	<p>Source E does not prove that the views expressed in Source D are justified as it states that the Singaporean government has been vigilant, as it has taken measures to invest in cyber security. This is seen in “With that level of technology and success comes plenty of cyber defence systems, and it is clear that the government has spared no expense on this. This shows that the Singapore government has invested all they could to ensure that they had the best technology in combating cybercrime. This is different from Source D’s view that the government has been lax in their management of cybersecurity issues. It says that “the initial government response to the largest cyberattack in Singapore was slow and inadequate”, and “it is apparent that more could have been done to deter the cyber-attack, but no action was carried out.” This shows that the government was not sufficiently prepared, such that a major attack could happen where Singaporeans’ personal details were obtained by the cyber-criminals. Thus, since Source E challenges Source D, it does not prove that the view that the government is not prepared for cyberattacks is justified.</p>	
L5	<p>L4 + Proves/Does not prove based on CR, supported <i>Award 6 marks for well-explained and supported answers on both sides</i></p> <p>Source E proves that the view expressed in Source D regarding the need to educate Singaporeans is justified, since Source B shares Source E’s views on the need to educate negligent individuals. Source D states “I think the government needs to increase their efforts to educate the people on the importance of cyber-security in today’s time.” This shows that Source D believes that governments need to ensure that the citizens are sufficiently informed about the threat posed by cybercrime. Similarly, Source E states, “To better protect the cyber system, Singaporeans need to be educated sufficiently regarding the threats of cyber-attacks”, which shows that Source E believes that Singaporeans need to be taught the consequences of cyber-threats. This is supported by Source B, which states, “SME leaders are beginning to recognize the importance of better training in cyber risk management, with 58% identifying it as an important next step”. This shows that SME leaders understand that in order to minimise employee negligence, it is important for companies to take the steps to educate them on the consequences of cyber threats. Since Source B supports Source E, Source E proves that Source D’s view on the need to educate Singaporeans is justified.</p>	[5-6]

Source E **does not prove that the view expressed in Source D regarding the readiness of the government is justified**, since Source F shares Source E's views on the capability of the government in dealing with cybersecurity issues. This is seen in "With that level of technology and success comes plenty of cyber defence systems, and it is clear that the government has spared no expense on this. This shows that the Singapore government has invested all they could to ensure that they had the best technology in combating cybercrime. **This is different from Source D's view that the government has been lax in their management of cybersecurity issues.** It says that "the initial government response to the largest cyberattack in Singapore was slow and inadequate", and "it is apparent that more could have been done to deter the cyber-attack, but no action was carried out." **This shows that the government was not sufficiently prepared, such that a major attack could happen where Singaporeans' personal details were obtained by the cyber-criminals. However, Source E is supported by Source F**, which states, "Singapore has more centralised controls to prepare for cyber incidents and respond to them than the United States, and potentially any nation out there." **This shows that the Singapore Government's has always had the capability to deal with cyber incidents due to its power to regulate and police cyberspace in Singapore. Since Source F supports Source E, Source E does not prove that Source D's view regarding the readiness of the government.**

L6

L4 + Proves/Does not prove based on Evaluation of Provenance of Source E, fully explained

Award 6 marks for Evaluation of Provenance of Source E + Similarity OR Difference between E and F

Award 7 marks for Evaluation of Provenance of Source E + Similarity AND Difference between E and F

Source E **proves that the view expressed in Source D regarding the readiness of citizens is justified**, since Source E can be regarded as an authoritative source on cybercrime, and is therefore reliable in this context. Since Source E is an online technology magazine that focuses on trends and developments in cyber technology, we can regard what it says on the readiness of **citizens** to be true, since it would have had the resources, expertise and research to draw **such conclusions**. Source D states "I think the government needs to increase their efforts to educate the people on the importance of cyber-security in today's time." This shows that **Source D believes that**

[6-7]

governments need to ensure that the citizens are sufficiently informed about the threat posed by cybercrime. This is supported by Source E, which says “To better protect the cyber system, Singaporeans need to be educated sufficiently regarding the threats of cyber-attacks”, which shows that **Source E believes that governments need to teach Singaporeans regarding the consequences of cyber-threats. Thus, since Source E is reliable and supports Source D, it proves that the view on the need to educate Singaporeans is justified.**

Source E **does not prove that the view expressed in Source D regarding the readiness of the government is justified**, since Source E can be regarded as an authoritative source on cybercrime, and is therefore reliable in this context. Since Source E is an online technology magazine that focuses on trends and developments in cyber technology, we can regard what it says on the readiness of the **government** to be true, since it would have had the resources, expertise and research to draw such conclusions. This is seen in “With that level of technology and success comes plenty of cyber defence systems, and it is clear that the government has spared no expense on this. This shows that the Singapore government has invested all they could to ensure that they had the best technology in combating cybercrime. **This is different from Source D’s view that the government has been lax in their management of cybersecurity issues.** It says that “the initial government response to the largest cyberattack in Singapore was slow and inadequate”, and “it is apparent that more could have been done to deter the cyber-attack, but no action was carried out.” **This shows that the government was not sufficiently prepared, such that a major attack could happen where Singaporeans’ personal details were obtained by the cyber-criminals. Thus, since Source E is reliable and challenges Source D, it does not prove that the view that the government is not prepared for cyberattacks is justified.**

4	Study Source F.	[6]
	Is this source surprising? Explain your answer.	
L1	Surprised OR/AND Not Surprised, superficial analysis	[1]

	<p>Source F is surprising because he did not cancel the summit after Singapore encountered a huge failure in their cybersecurity measures.</p>	
L2	<p>Surprised OR/AND Not Surprised based on provenances of interviewees in Source F, undeveloped, OR Surprised OR/AND Not Surprised, valid analysis, unsupported <i>Award 2m for Surprised OR Not Surprised with unexplained provenance</i> <i>Award 3m for Surprised AND Not surprised with unexplained provenance</i></p> <p>Source F is not surprising as it is expected for him to comment on cybersecurity in Singapore, since he is the CEO of a cybersecurity firm.</p> <p>Source F is surprising as it is unexpected Mr Mandia declined to comment on a major attack in Singapore.</p>	[2-3]
L3	<p>Surprised OR/AND Not Surprised based on Source F content, supported <i>Award 3m for Surprised OR Not Surprised, supported by source details from F, with contextual development</i> <i>Award 4m for Surprised AND Not Surprised, supported by source details F, with contextual development</i></p> <p>Source F is surprising as it is unexpected Mr Mandia declined to comment on a major attack in Singapore given that he had been in Singapore for a Cyber Defense Summit. Source F states, “when asked, Mr Mandia declined to comment specifically on the SingHealth hack in July 2018 - which was described as Singapore's most serious breach of personal data”. This is surprising given that he was in Singapore for this company’s Cyber Defense Summit and would therefore be expected to address such a major cyber security lapse.</p> <p>Source F is not surprising because it is expected for Mr Mandia to praise Singapore, given that Singapore has the capabilities to deal with cybercrime. Source F states, “Singapore can play an important role in cybersecurity for Southeast Asia ... Singapore has more centralised controls to prepare for cyber incidents and respond to them than the United States, and potentially any nation out there”. This shows that he recognises that Singapore is even better equipped to deal with cyber threats than the United States, due to its ability to coordinate operations within the country.</p>	[3-4]

L4	<p>Not Surprised based on Source F, with Cross-reference <i>Award 5m Not Surprised, supported with cross-reference,</i></p> <p>Source F is not surprising because it is expected that Mr Mandia plays Singapore up as a leader in cyber-security in Southeast Asia. Source F states, “Mr Kevin Mandia felt that Singapore can play an important role in cybersecurity for Southeast Asia, it can lead the way for others in the region in terms of how to respond to cyber incidents, and coming up with cyber rules for the region should it want to.” This shows that he believes Singapore can lead by example in Southeast Asia, for other countries in the region to follow, in combating cybercrime as it has the resources to do so. This tallies with my expectations from Source E, which states, “Singapore is the major technology hub of Southeast Asia. With that level of technology and success comes plenty of cyber defence systems, and it is clear that the government has spared no expense on this.” This shows that Source E also recognises Singapore as a regional leader in cybersecurity. Since Source F tallies with Source E, I am not surprised.</p> <p>Accept CR to Source D for “surprise” CR must be to sources that allude to Govt’s ability to manage cyber-security</p>	[5]
L5	<p>Not Surprised by Mr Mandia declining to comment due to the context of the interview</p> <p>Source F is not surprising because it is expected for Mr Mandia to decline to comment due to the context of the interview. Source F states, “when asked, Mr Mandia declined to comment specifically on the SingHealth hack in July 2018 - which was described as Singapore's most serious breach of personal data”. This might seem surprising given that he was in Singapore for this company’s Cyber Defense Summit and would therefore be expected to address such a major cyber security lapse. However, on the whole, since Singapore hosted the summit for that year, he might not have felt comfortable with making negative comments on Singapore’s cybersecurity, for fear of potential backlash. It is also entirely possible that he had been approached by the authorities not to discuss the event. As such, it would not be surprising that he declined to comment, given that he had a potential motive for doing so.</p>	[6]

5	<p>“It is the individual’s responsibility to manage cybercrime.” Using sources in this case study, explain how far you would agree with this statement.</p> <ol style="list-style-type: none"> 1. Students did not manage to complete the paper. Time management was a challenge for some students, and some did not write answer the question. As such, there were instances where answers were just incomplete or did not use any source in a valid manner as the statements were very generic in nature. Some students wrote only the answer for the "agree" portion and did not write anything for the "disagree" portion. Remember the Evaluation question needs to be handled in a balanced manner. 2. Some students did not answer the question. It is important to remember that you need to answer the question stem and explain clearly your reasons for agreement or disagreement with the source. The question asked “Using sources in this case study, explain how far you would agree with this statement.” The following shows the typical answers: <ul style="list-style-type: none"> • Source A disagrees as individuals should be responsible. -> Are you Source A? [Remember this only applies for History!] • Source A shows that there is a bomb threat because individuals did nothing about it. -> Answer the question, so do you agree / disagree? Don’t make the marker guess like a bomber man): 3. Students frequently misinterpreted a number of sources in their analysis. It is important to remember that when you analyse each source, it should be done holistically, do not use 1-2 sentences to determine the interpretation of each source. 4. For students who did manage to write an answer for Q5 but their explanations were insufficient. In this case, students combined their explanations for multiple sources and the explanation fell flat for all 2-3 sources. Such answer typically looked like this: <ul style="list-style-type: none"> ○ "I agree that individuals should be responsible. Source A shows that... Also, Source C states that "... Furthermore, Source E states that "... <u>All three</u> 	[10]
---	---	------

sources show that the individuals have to do something and make sure they are doing it right.

- The biggest problem here was that the single explanation did not sufficiently cover all **THREE** pieces of evidence for the different aspects provided. In fact, the explanation typically does not even seem to refer to specific details quoted in the evidence. Remember to quote each piece of evidence and explain them in detail. Do not lump them together due to the lack of time, remember **QUALITY supersedes QUANTITY**.
 - In such cases, what students should have done was quote and then explain each source separately. E.g.:
 - "I agree that individuals should be responsible for managing cybercrimes. Source A shows that... **This means that...** Also, Source C states that "... " **Source C is saying that..** Furthermore, Source E states that "... **This implies that...**"
 - It is important to explain your answer to demonstrate two key areas to adequately address the statement. 1. Agency [Who is involved? If not Individuals, then who?] 2. Actions [What did they do to demonstrate that they were responsible in managing cybercrimes?]
5. For the **balanced conclusion**, answers need to have properly explained **BOTH** sides for it to count. Otherwise, the argument is not balanced at all. Remember that there are different kinds of conclusions:
- A **SUMMARY** is a simple listing of what has already been said. It is a recap and does not add anything to the argument.
 - An **EVALUATION** is a higher-level answer as it considers both sides of the argument and **then explains which is the stronger side and WHY**.
6. For the **assessment of Reliability/Usefulness**, remember that you cannot use sources that have already been used/assessed before. As such, evaluation of Reliability of D and E cannot be accepted.
7. Several answers used **contextual knowledge** from their own personal experiences, and this was acceptable in

	<p><i>most cases. However, there were some cases that were very subjective, and these examples were problematic as they tended to make the fallacy of false generalisations or blanket statements. E.g.:</i></p> <ul style="list-style-type: none"> ○ <i>“My friend uses a simple password even though we learnt that we should use complex password. Hence, individuals should be responsible, so I agree with the statement.”</i> <p><i>The above statement is problematic because it generalises that from her friend’s experience to infer the responsibility of individuals? In what ways did the friend manage cybercrime?</i></p>				
L1	Writes about statement, no valid source use	[1]			
L2	<p>Yes OR No, supported by valid source use</p> <p><i>Award 2m for using only 1 source</i> <i>Award 3m for using only 1 source and with good explanation</i> <i>Award 3m for using at least 2 sources</i> <i>Award 4m for using at least 2 sources and with good explanation</i></p>	[2-4]			
L3	<p>Yes AND No, supported by valid source use</p> <p><i>Award 5m for both Yes and No, with only 1 source on <u>each</u> side</i> <i>Award 6m for both Yes and No, with at least 2 sources on <u>one</u> side</i> <i>Award 7m for both Yes and No, with at least 2 sources on <u>each</u> side</i> <i>Award 8m for both Yes and No, with at least 2 sources on <u>each</u> side and good explanation</i></p> <p>To score additional 2m, candidates can use any of the following methods:</p> <ul style="list-style-type: none"> • Analysing at least 1 source in its usefulness, reliability or sufficiency <ul style="list-style-type: none"> ○ Answers from previous questions cannot be accepted. ○ Evaluation of Reliability of D and E cannot be accepted. • Sharing examples from their contextual knowledge • By giving a balanced conclusion or resolution <p><i>Award 1m for any one of the above</i> <i>Award 2m for more developed answers</i></p> <p>E.g.</p> <table border="1"> <tr> <td>Source</td><td>Agree</td><td>Disagree</td></tr> </table>	Source	Agree	Disagree	[5-8]
Source	Agree	Disagree			

A	Steps need to be taken by individuals to secure their wireless networks so that it is not used for cybercrime.	
B	Individuals need to be careful not to commit administrative errors or lose sensitive information that would make their company vulnerable to cybercrime.	Companies should recognise the increasing danger cybercrime poses to businesses, and take necessary precautions, such as training their personnel and communicating clearly to their employees on the dangers of cybercrime. Thus, it is the responsibility of companies.
C	Individuals need to ensure that they are vigilant and not fall victim to cyber-scams.	
D	It is necessary for citizens to ensure that they take precautions against cybercrime by using strong passwords.	The government should respond quickly to cyberattacks when they happen, and also educate its employees on proper security protocols, showing that it is their responsibility.
E	The most stringent cybersecurity measures are meaningless if people are not sufficiently educated to be vigilant, showing that it is the responsibility of individuals to ensure that networks remain secure from cybercrime.	The Singapore government has prioritised spending on cybersecurity, showing that it recognises the government's responsibility in combating cybercrime.
F		Mr Mandia commented that the Singapore government can play an important role as a regional leader in dealing with cyber threats. This shows that he believes it to be the responsibility of the Singapore government to combat cybercrime in the region.

Using reliability

Source A can be regarded as a reliable source on combating cybercrime as it was first created by the IDA of Singapore, and they would have the knowledge on the latest cybercrime trends. Additionally, this was published by a department in a university that specialises in IT solutions for its students and faculty. This means that it has the expertise on the latest cybercrime trends, especially those affecting university students. As a result, its advice on cybercrime is likely grounded in facts. It is likely that has specifically chosen this cartoon as a way to convey its warning, showing that it has curated the information and recognised it to be a relevant way to engage its audience. Because of this, we can regard this as a useful source regarding the importance of securing home networks, thereby making it sufficient for us to conclude, with this source alone, that individuals have a responsibility in combating cybercrime.

Contextual Knowledge

Overall I agree with the statement as there are now more measures that individuals can adopt to ensure the safety of private data, such as 2-factor authentication, that offers an additional layer of protection even when passwords are compromised. For example, in many online services these days, such as Google, they give you an option of turning on 2-factor authentication that is connected to your mobile phone. When turned on, any log-in on your Google account will lead to a prompt on your mobile phone, which needs to be approved in order for the log-in to be successful. This will ensure that only you have access to your account, even if your password has been compromised by a data breach. This thus adds an added layer of responsibility on the individual, such that even if data breaches happen, the individual's data continues to be protected.

Balanced Conclusion

Overall, I would agree that it is the individual's responsibility to adopt good cybersecurity practices so that criminals do not gain access to sensitive data for misuse. As mentioned in Sources B and D, there are many vulnerabilities that hackers can exploit, such as poor passwords and lax practices that individuals have the power to address. While it is possible for the government and companies to educate citizens on the importance of good cybersecurity practices as seen in Sources D and E, these warnings will be ineffective if individuals do not heed them, as seen in Source E. As such, the individual is the determining factor that ultimately decides how effective these government advisory campaigns are. Thus, overall, I agree with the statement.

Overall, I would disagree that it is the individual's responsibility since there are events that are beyond the individual's control, such as major data breaches. As mentioned in Source D, there are cases where customer records have been left unprotected, that could have been addressed if SingHealth had been more vigilant about their protocols. Since SingHealth is a Government healthcare organisation which many individuals have come to rely on for healthcare, it may not be within the individual's power to choose a different alternative. As such, it becomes the government organisation's responsibility to ensure that the data breaches do not happen by protecting such information properly.

Section B

Question	Answer	Marks
6	<p>Extract 1 shows an example of an incident that led to a “brownface” controversy in Singapore.</p> <p>What important ideas would you promote to reduce the occurrence of similar incidents? Explain your answer with reference to two ideas.</p>	[7]
L1	Describes the topic	[1]
L2	<p>Identifies / Describes ideas <i>Award 2m for identifying one idea</i> <i>Award 3m for identifying two ideas</i> <i>Award 3m for describing one idea</i> <i>Award 4m for describing both ideas</i></p>	[2-4]
L3	<p>L2 + Explains ideas <i>Award 5-6m for explaining one idea</i> <i>Award 6-7m for explaining two ideas</i></p> <p>Note: An explanation is showing how the idea led to ...</p> <p>One idea I would promote to maintain harmony would be for Singaporeans to be mindful of their speech, their actions and be sensitive towards the feelings of other races. For instance, hurtful comments that direct towards the other race’s skin colour, language, behaviour should be avoided. A possible platform to promote such an idea could be via educational campaigns. For example, Singapore has the Singapore Kindness Movement where Singaporeans are inspired to be gracious by doing kind acts to others. Through such educational campaigns, Singaporeans would understand the significance of hurtful comments and start to understand there are many commonalities among us despite the differences in race sending the message that we are actually the same in essence and that no race will condone any negative value such as violence to its followers. In this way, greater understanding among Singaporeans is forged and will help ease acceptance of the differences in our society forging racial harmony in Singapore. By doing so, Singaporeans can avoid conflict as they do not make hurtful remarks that may damage the relationship between Singaporeans which aids in maintaining harmony in Singapore. Hence, when Singaporeans take note of what they say and do, we can maintain racial harmony as we do not make hurtful remarks towards other races that reduces the probability of conflicts.</p> <p>Another idea I would promote to maintain harmony would be for Singaporeans to be open to learn about each other’s cultural differences and practices. For instance, Singaporeans can take part in each other’s celebration at various common spaces like the community</p>	[5-7]

	centres. The Chinese can join the Malays' Hari Raya celebrations so that they know how it is celebrated. The Malays can also invite their neighbours of other races to their wedding so that they can understand their cultural practices. This helps to promote greater racial harmony as the different races will be able to come together to spend time, interact and develop social bonds and connections. Through these positive interactions, they will better understand each other and may continue to sustain the friendships forged. This will eventually lead to greater racial harmony due to the positive relations and trust created among the racial groups.	
--	---	--

Question	Answer	Marks
7	Extracts 2 and 3 reflect on assimilation and integration as approaches to manage socio-cultural diversity. Do you think that integration is more effective in managing socio-cultural diversity than assimilation? Explain your answer.	[8]
L1	Writes about the topic but without addressing the question.	[1-2]
L2	Describes the part played by factors <i>Award 3m for describing one factor</i> <i>Award 4m for describing both factors</i>	[3-4]
L3	Explains the part played by factors <i>Award 5-6m for explaining one factor</i> <i>Award 6-7m for explaining both factors</i> Note: <ul style="list-style-type: none"> • 1-2 well-explained examples will suffice. • Answers which are too narrow and only focus on one context should be considered weak explanations. • An explanation is showing how the factor is related to increasing diversity in Singapore. <p>Assimilation is effective in managing socio-cultural diversity. Assimilation policies mean that immigrants are expected to adopt the beliefs and practices of the majority group. Over time, this is supposed to make the identity of the immigrants indistinguishable from the majority group in aspects such as cultural beliefs and practices. For example, in France, education is secular. There is no discussion about religion except in History and Philosophy classes. Adaptation classes are also conducted for the children of immigrants to help them improve their French and eventually join regular French schools. With a common language and culture, there will be a common basis for understanding which will lead to greater harmony in the society. Misunderstandings and tension are not likely to occur. Moreover, with the expectation that all French citizens identify with the principle of secularism, and that diversity does not overshadow national identity</p>	[5-7]

	<p>that binds all French citizens, France achieves the policy of national identity and harmony in the society.</p> <p>Integration is effective in managing socio-cultural diversity. Integration policies mean that immigrants retain their unique identities while forging common ground with the groups already living in the host country. For example, Singapore practices the policy of Bilingualism which requires all students to learn English and their Mother Tongue. English serves as a common language of communication to foster sense of belonging and promote integration while Mother Tongue allows the preservation of cultural identity and heritage. With the growing diversity in Singapore, integration is emphasised through promoting equality without granting special rights to any particular racial, ethnic or religious group. Integration is also achieved when diverse socio-cultural identities complement the national identity of being a Singaporean with their unique identities. In this manner, no group is excluded because everyone can be unique yet uphold the identity of being a Singaporean. Hence, this leads to a harmonious society.</p>	
L4	<p>Both aspects in L3 plus explains the relative importance of each factor</p> <p>Note: A balanced conclusion will assess the merits of each fact and show the relative importance between the two. Do not accept answers that only focus on one factor and leave out the other.</p> <p>In conclusion, I think that integration is more effective in socio-cultural diversity than assimilation. When assimilation is used, immigrants are forced to relinquish their own cultures and practices. This might cause some new immigrants' discomfort when doing so. Furthermore, should a local see an immigrant behaving slightly differently, they might think that the immigrant is up to no good, and this might cause tensions to arise. However, when integration is adopted, the immigrants are able to preserve their culture and this would lead to better understand the various groups in the country leading to a more harmonious society. Thus, integration is more effective in managing new immigrants into a country.</p>	[8]