Class:	Register No:	Name:

CRESCENT GIRLS' SCHOOL
SECONDARY FOUR
PRELIMINARY EXAMINATION 2021

COMBINED HUMANITIES

2272/1
2273/1
2274/1

Social Studies

24 August 2021

1 hour 45 mins

READ THESE INSTRUCTIONS FIRST

Write your name, class and register number on your answer paper.
Write in dark blue or black pen on both sides of the paper.
Do not use staples, paper clips, glue or correction fluid.

Section A
Answer **all** questions.

Section B
Answer **both** questions.

At the end of the examination, fasten the answers to Section A and Section B **separately**.

The number of marks is given in brackets [ ] at the end of each question.

This paper consists of **8** printed pages (including the cover page).

Section A (Source-Based Case Study)

Answer **all** questions.

Exploring Citizenship and governance

Study the Background Information and the sources carefully, and then answer all the questions.

You may use any of the sources to help you answer the questions, in addition to those sources which you are told to use. In answering the questions, you should use your knowledge of the topic to help you interpret and evaluate the sources.

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]**

2 Study Sources B and C.

How similar are the two sources?
Explain your answer.

[7]

3 Study Source D and E.

How far does Source E prove that the views expressed in Source D are justified? **[7]**
Explain your answer.

4 Study Source F.

Is this source surprising? Explain your answer. **[6]**

5 "It is the individual's responsibility to manage cybercrime."

Using sources in this case study, explain how far you would agree with this statement. **[10]**

[Turn Over

How prepared is Singapore to deal with cyber-crime?

BACKGROUND INFORMATION

Read this carefully. It may help you to answer some of the questions.

Singapore has long had a reputation for being a leader in cybersecurity in Southeast Asia, having been a major technology hub in the region.

However, some major data breaches in government systems have undermined Singapore's capabilities in dealing with cybercrime. In July 2018, a high-profile data breach happened in Singapore, during which the national healthcare system database, SingHealth, was hacked and the personal particulars of 1.5 million patients were stolen. Singapore has since responded by heightening cyber-security, but data-breaches continue to happen.

Read the following sources to find out if Singapore is prepared to deal with cyber-crime.

Source A: *A cartoon commissioned by the Infocomm Development Authority of Singapore, published on a university technical support department web page.*

Source B: *An excerpt from a report published by Chubb Asia Pacific, titled "Singapore *SME Cyber Preparedness Report 2019", published in 2020. Chubb is one of the world's largest cyber insurers, which are insurance companies that offer compensation to victims of cyber incidents.*

*SMEs reported a rise in cyber incidents from 2018 to 2019. Yet, they seem less worried about the impact on their business compared to last year. This is worrying, as complacency invites malicious attacks, future breaches and inadequate incident response.

SME leaders also have a poor opinion of their employees' readiness against cyber incidents. This is unsurprising. Just over half (53%) of the cyber incidents that SMEs suffered in the past 12 months were caused by employees – either through administrative errors (30%) or through the loss or theft of a company device such as a laptop or USB drive (23%).

However, placing the blame solely on employees is not the answer. Fortunately, SME leaders are beginning to recognize the importance of better training in cyber risk management, with 58% identifying it as an important next step. Almost half also recognise that there should be clearer communication from the management to employees about the importance of cyber security.

SME: Small-Medium Enterprise – a small local business. They are different from Multi-National Corporations, whose operations span multiple countries.

Source C: *An excerpt from survey findings conducted by Microsoft, a technology company, on consumers' vulnerability to technical support scams, which is a type of online scam, published online on 29 October 2018.*

According to the survey, fewer consumers in Singapore have encountered a technical support scam in 2018 as compared to 2016. 57 percent of consumers said that they have encountered a technical support scam, which is a decline from the 65 percent who encountered one in 2016.

While over half of Singaporeans have encountered a technical support scam in the past year, Singapore is ranked among the most savvy countries globally when dealing with technical support scams. 43 percent of Singapore respondents chose not to interact with scammers – the fourth highest in the world.

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.

Source D: *An excerpt from a post in the "comments" section of an article in a local online newspaper on the SingHealth data breach, published on 21 September 2018.*

When the breach first happened and was first announced, many were concerned about its implications. However, the initial government response to the largest cyberattack in Singapore was slow and inadequate. The SingHealth staff were not aware of the weaknesses happening in the software system that SingHealth utilises for its electronic medical records. It is apparent that more could have been done to deter the cyber-attack, but no action was carried out.

Another common problem is the use of a common and weak password which can be easily cracked by the attacker to gain access to the account. Despite all of the efforts done by the government to ensure cyber security, how did this happen? I think the government needs to increase their efforts to educate the people on the importance of cyber-security in today's time.

Source E: *An excerpt from an article published in an online technology magazine on 5 April 2019. The magazine is focused on trends and developments in the cyber technology in Southeast Asia.*

Recently, Group-IB* announced that it had discovered login details of Singaporean government and education employees plus more than 19,000 Singaporean bank cards' details on the Dark Web**. 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.

However, without sufficient 'peopleware', the best software and hardware is essentially redundant. The apparent cause is the Singaporean mindset when it comes to cybersecurity.

To better protect the cyber system, Singaporeans need to be educated sufficiently regarding the threats of cyber-attacks, while companies themselves need to work alongside gold-standard security firms to improve their software and cover any loopholes.

*Group-IB: A global cybersecurity organisation partnered with Interpol, an international police organisation
**Dark Web: A hidden part of the internet that requires special software to access. It facilitates cybercriminal activity.

[Turn Over

Source F: *A report of comments made by Mr Kevin Mandia during an interview conducted while he was in Singapore, published on 5 October 2018. Mr Mandia is the CEO of FireEye, an American cybersecurity firm. He had been in Singapore for the Cyber Defense Summit – an annual event organised by his company, where participants share ideas and discuss developments in cybersecurity.*

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. Singapore has more centralised controls to prepare for cyber incidents and respond to them than the United States, and potentially any nation out there. And Singapore is organised; it is a nation that does what it says it will do.

However, 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. 1.5 million patients' non-medical personal data were stolen, including Prime Minister Lee Hsien Loong's - as well as how the Government responded in disclosing the incident to the public.

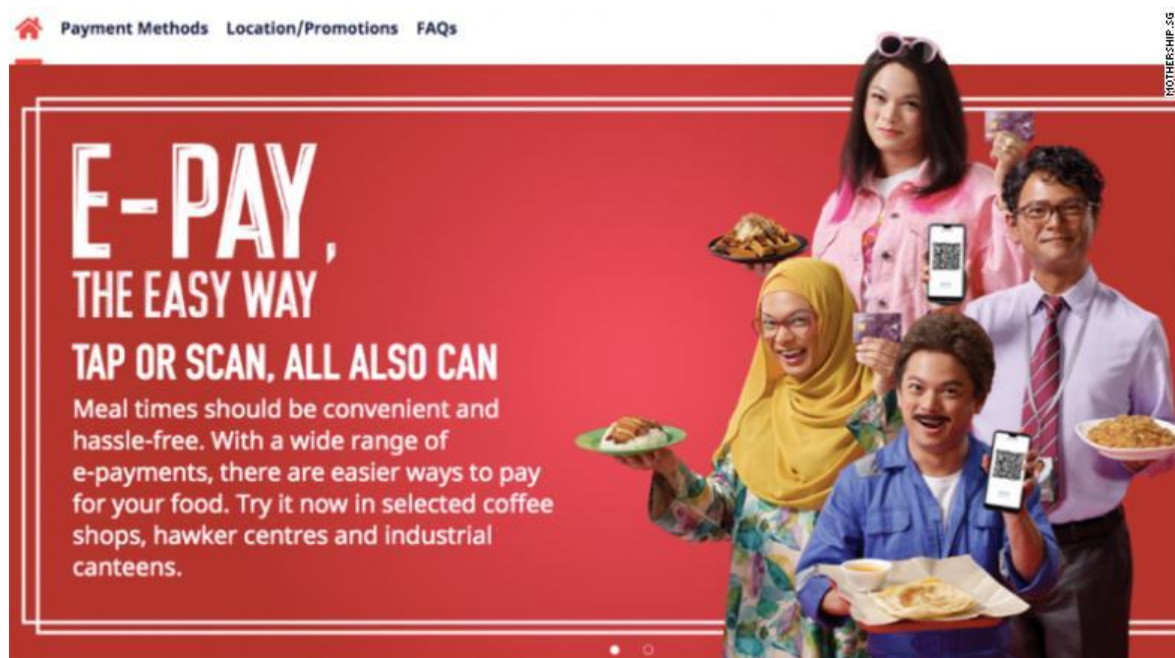## SECTION B (Structured-Response Questions)

Answer **both** questions.

Living in a Diverse Society

Study the extracts carefully, and then answer the questions.

Extract 1

In 2019, an ethnically Chinese actor who allegedly darkened his skin to portray characters of different races in an advertisement sparked a "brownface" controversy in Singapore.

Extract 2

In France, they adopt a policy of assimilation guided by the principle of *laïcité*, which means secularism—where there is no religious involvement in government affairs. Hence, it is expected for the French population to identify with common French national values.

Extract 3

In Singapore, we adopt a policy of integration where differences are recognised and respected. Hence, cultural diversity forms a part of Singapore's national identity, where immigrants readily integrate into our society.

[Turn Over

6	Extract 1 shows an example of an incident that led to a "brownface" controversy in Singapore.

What important ideas would you promote to reduce the occurrence of similar incidents? Explain your answer with reference to **two** ideas.	[7]

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]

END OF PAPER