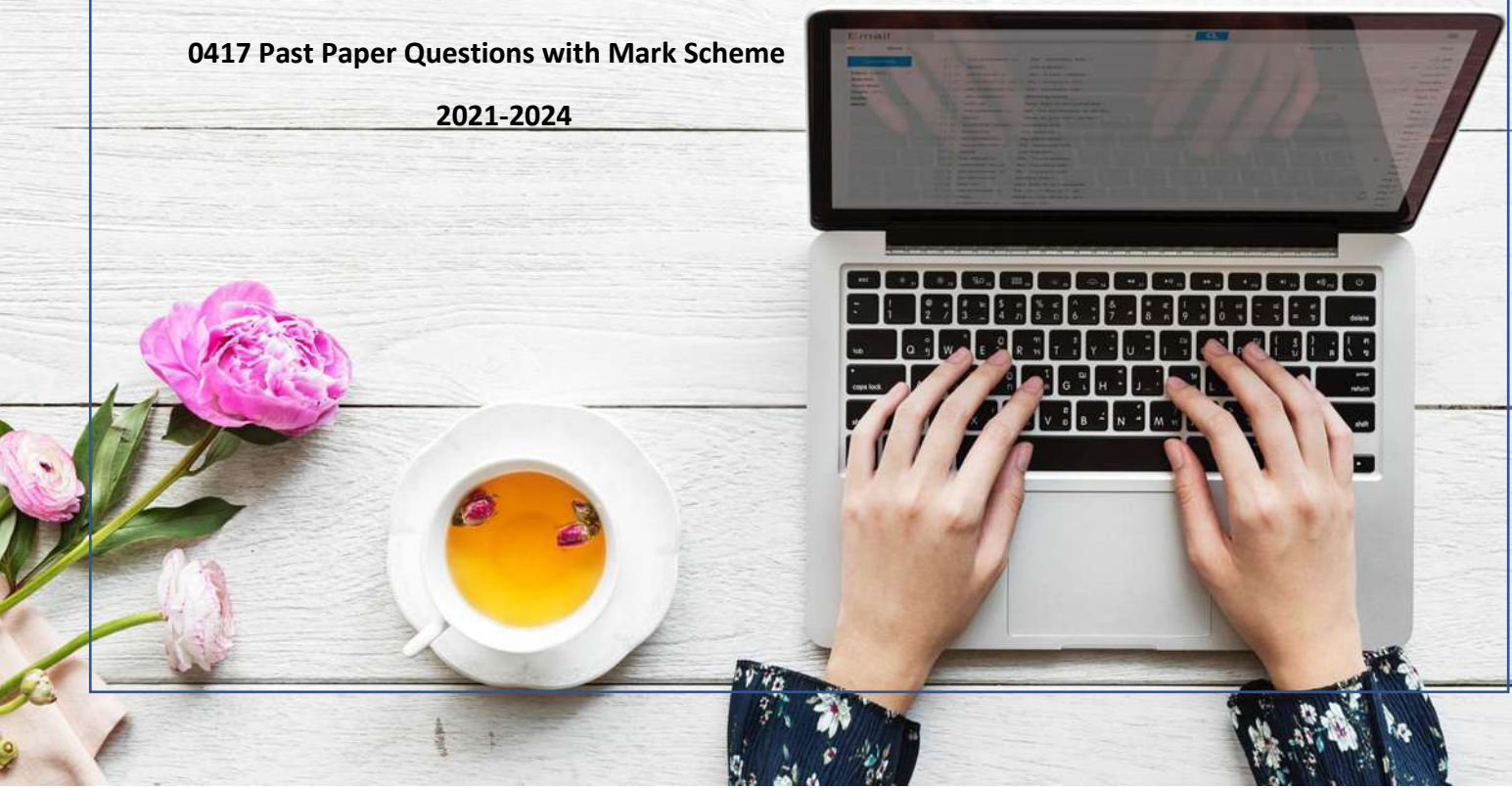
Information and Communication Technology

-0417-

Chapter Eight: Safety and Security

0417 Past Paper Questions with Mark Scheme

2021-2024



1 A parent is concerned about his children sending texts. When sending a text, it is important to follow netiquette.

(a) Explain what is meant by the term netiquette.

.....

.....

.....

..... [2]

(b) The parent is planning to produce a number of rules to ensure that his children follow netiquette when texting other people.

Write down **four** rules that he could include in his list.

1.....

.....

2.....

.....

3.....

.....

4.....

.....

[4]

2 A company has placed a firewall between their Local Area Network (LAN) and their internet connection. This is used to increase security in their computer systems.

Discuss the effectiveness of using this firewall to increase security.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

[6]

3 Tick (✓) whether the following are examples of personal data.

	Yes (✓)	No (✓)
Full name		
Capital of England		
Gender		
Number of flowers in a garden		

[2]

4 Complete the sentences below using the most appropriate word from the list.

cookies	hacking	pharming	phishing
smishing	spam	spyware	virus

(a) The act of gaining unauthorised access to a computer system is called

..... [1]

(b) The software that gathers data by monitoring key presses on a user's keyboard is called

..... [1]

(c) A fake text message, that could contain a link, sent to a mobile phone is called

..... [1]

5 Students often use IT equipment; therefore it is important to have a good physical safety strategy.

Evaluate your own use of IT equipment, in terms of physical safety, and describe the strategies you will need to minimise the potential physical safety risks.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

6 When an email is sent, it could have a digital certificate attached.

Explain why a digital certificate is required. Include in your answer items that could be found in a digital certificate.

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [5]

7 One way of communicating with other people is to use emails. It is very important that when you send and receive emails you are aware of esafety.

Evaluate your own use of email in terms of esafety and describe the strategies you will need to minimise the potential esafety risks.

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

.... [8]

8 Many young people play online games. One problem with online gaming is that it is easy to give out personal details accidentally. Some users create weak passwords which could lead to their personal details being accessed.

(a) Name **two** pieces of personal data that could be accessed.

1 .....

.....

2 .....

.....

[2]

(b) Write down **three** rules that should be applied when setting a strong password.

.....

.....

.....

.....

.....

.....

[3]

(c) Describe safety measures that should be taken by gamers to ensure their data is safe other than using strong passwords.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

9 The Internet of Things (IoT) is a computer network which allows users to control household devices remotely. It has many benefits, for example a user can turn on the house central heating via a smartphone. The IoT can use WiFi and Bluetooth which can cause problems regarding data security.

Describe the methods that could be taken to protect the user's data.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

10 Students in Tawara College are using the internet to find information for a project. They have been told that the college has a firewall.

(a) Explain what is meant by a firewall and why it is used.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

The students visit different websites to get information for their project.

(b) Explain why it is **not** always easy for the students to find reliable information on the internet.

.....

.....

.....

.....

.....

.....

.....

..... [4]

11 Keeping data secure is very important in any computer system. Many organisations use encryption when sending data.

(a) Describe the term encryption.

.....

.....

.....

.....

.....

.....

.....

..... [4]

(b) Another way of protecting data in a computer system is to use passwords.

Identify methods to prevent hackers from gaining knowledge of someone's password.

.....

.....

.....

.....

.....

.....

.....

..... [4]

12 Circle **two** items that contain personal data.

bank card	bar code	laser printer
medical record	mouse	sensor

[2]

13 Many company computer network systems use WiFi as a communication system to help prevent the issue of tripping over trailing cables.

(a) For each of the following physical safety issues describe **two** ways of helping to prevent them.

(i) Fire

Prevention 1 .....

.....

Prevention 2 .....

.....

[2]

(ii) Electrocution

Prevention 1 .....

.....

Prevention 2 .....

.....

[2]

A common use of home computers is online gaming.

(b) Describe **three** eSafety measures which should be taken when playing games on the internet.

1 .....

.....

2 .....

.....

3 .....

.....

[3]

(c) In order to log onto online gaming a user ID and password is needed.

Explain what is meant by a user ID and password and why they are needed.

.....

.....

.....

.....

.....

.....

.....

..... [4]

14 A patient has an injury and the doctor treating him needs to find out information about the patient. Most of the data he needs to collect is personal data.

The data collected is protected by data protection legislation. Most data protection acts include the principle that data should be kept confidential and secure.

(a) List **four** other principles of a typical data protection act.

1 .....

.....

2 .....

.....

3 .....

.....

4 .....

.....

[4]

(b) Explain what is meant by personal data. Include **two** examples of personal data in your answer.

Explanation .....

.....

.....

.....

Example 1 .....

.....

Example 2 .....

.....

[3]

(c) Explain why personal data should be kept confidential and secure.

.....

.....

.....

.....

.....

.....

.....

..... [4]

15 Computers can store data in the cloud rather than using storage devices in the computer.

(a) Describe **three** benefits of storing data in the cloud.

1 .....

.....

2 .....

.....

3 .....

.....

[3]

(b) Describe **three** drawbacks of storing data in the cloud.

1 .....

.....

2 .....

.....

3 .....

.....

[3]

16 The protection of personal data is important as many transactions are carried out online.

(a) Explain how to avoid inappropriate disclosure of personal data.

.....

.....

.....

.....

.....

.....

.....

..... [4]

(b) Controlling the freedom of speech is part of policing the internet.

Discuss whether the internet should be policed or not.

.....

.....

.....

.....

.....

.....

.....

..... [4]

17 There have been major issues regarding the accuracy of facial recognition systems for identifying suspects by the police.

Tawara Airport has installed biometric security including facial recognition systems to help the police recognise known criminals entering and leaving the country. Previously video was taken of all passengers and then checked manually.

(a) Discuss the effectiveness of using facial recognition systems rather than the manual video system to increase security in this way.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [8]

(b) Give **three** examples of biometric data.

1 .....

2 .....

3 .....

[3]

18 Instant messaging involves users sending text messages to each other.

Evaluate how you would use eSafety strategies in your own use of instant messaging.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

19 Due to data protection laws, personal data should be kept confidential and secure.

Explain why personal data should be kept confidential and secure.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

20 As our use of the cloud increases, new ways of accessing it safely need to be developed.

The use of typed passwords is being replaced by biometric methods.

Discuss the benefits and drawbacks of using biometric methods.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [8]

21 A company's computer system is protected by both a user ID and a password.

(a) Explain how a user ID and a password are used to increase the security of data.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

(b) The company plans to improve the security of its computer system by using biometric methods.

Describe what is meant by biometric methods. Give **two** examples of biometrics.

Description .....

.....

.....

.....

Example 1 .....

Example 2 .....

[4]

22 A student has been the victim of a vishing scam.

(a) Explain what is meant by the term vishing.

.....

.....

.....

..... [2]

(b) Describe **two** methods that help to prevent vishing.

1.....

.....

2.....

.....

[2]

23 Complete each of the following sentences.

(a) The scrambling of data being sent from one device to another device is called

..... [1]

Ch.1 **(b)** Using a computer to maintain the temperature of a room is called

..... [1]

(c) Unauthorised access to a computer system is called

..... [1]

Ch.7 **(d)** A conversation between a systems analyst and a member of staff that is part of the analysis is called

..... [1]

24 Roger is a 16-year-old student who is setting up a password for his computer. He has four ideas for the passwords he may use.

(a) Select the most appropriate password from the list and give reasons for your choice.

Roger2008

R08123

RogerZpa55w0rd

6lRrg08&

Password .....

Reasons .....

.....

.....

.....

[3]

(b) State **one** way of avoiding password interception.

.....

..... [1]

25 There are risks involved when using social networking sites.

Describe **four** strategies you could use to minimise the risks of using social networking sites to make new friends.

1 .....

.....

2 .....

.....

3 .....

.....

4 .....

.....

[4]

26 One of the threats to personal data is credit card cloning.

(a) Explain what is meant by credit card cloning.

.....

.....

.....

.....

.....

..... [3]

(b) One security improvement for this type of threat is the use of contactless cards.

Give **two** other security improvements that could be made to help reduce this type of threat.

1 .....

.....

2 .....

.....

[2]

27 A new patient is attending a medical centre. He completes a form with his details and gives this to the secretary who enters the details into a database.

Ch.15 **(a)** The secretary carefully checks the details entered into the database with those on the form.

State what this process is called.

..... [1]

(b) The medical centre follows a data protection act, so the patient's data is protected by law.

State **four** principles of a typical data protection act.

1 .....

.....

2 .....

.....

3 .....

.....

4 .....

.....

[4]

28 Remotely logging in to a college computer system requires two-factor authentication.

(a) Explain what is meant by two-factor authentication.

.....

.....

.....

.....

[2]

(b) State **two** examples of methods that could be used as part of two-factor authentication.

Example 1 .....

.....

Example 2 .....

.....

[2]

29 One of the risks when entering a password into a system is shoulder surfing.

(a) Explain what is meant by shoulder surfing.

.....

.....

.....

.....

[2]

(b) Give **two** security improvements that could be made to reduce shoulder surfing.

1 .....

.....

2 .....

.....

[2]

30 One of the risks when entering a password into a computer system is key logging.

(a) Explain what is meant by key logging.

.....

.....

.....

..... [2]

(b) Give **two** security improvements that could be made to prevent key logging.

1 .....

2 .....

[2]

31 The data on a computer system can be protected by anti-virus software and anti-malware software.

(i) Describe the features of anti-virus software.

.....

.....

.....

.....

.....

..... [3]

(ii) Describe the features of anti-malware software.

.....

.....

.....

.....

.....

..... [3]

32 Ensuring the privacy and confidentiality of data becomes more important when using computer networks.

Evaluate the different ways in which a user can ensure the privacy and confidentiality of data by using passwords.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Mark Scheme

Question	Answer	Marks
1a	**Two** from: Internet etiquette Set of social conventions They show common courtesy when communicating online	2
1b	**Four** from: Do not use capital letters as it relates to shouting Do not use abusive/vulgar language/threatening behaviour Be clear in the text sent Always check spelling and grammar Remember that sarcasm does not communicate well Respect other's privacy Respect other people's views Do not use too many emoticons Do not use text language/slang Do not spam Do not send inappropriate links	4

Question	Answer	Marks
2	**Six** from: *Benefits* Monitors traffic into and out of the network to make sure that all data passing is safe. Checks whether the data passing through it meets a given set of rules… …if they do not then the data is blocked Can block the unwanted traffic in and out of the network It can log all incoming and outgoing traffic to check later Can block certain undesirable websites/IP addresses Keeps a list of desirable IP addresses/websites It can block IP addresses to stop hackers *Drawbacks* It cannot stop individuals on internal networks by-passing the firewall It cannot stop employees hacking the computer from within the system Users own devices can by-pass the firewall therefore meaning the computer/network is in danger It cannot stop hackers only devices that hackers are using **To gain full marks on the question at least one benefit and drawback are needed**	6

<table>
<tr><th>Question</th><th>Answer</th><th>Marks</th></tr>
<tr><td>3</td><td>
<table>
<tr><th></th><th>yes</th><th>no</th></tr>
<tr><td>Full name</td><td>✓</td><td></td></tr>
<tr><td>Capital of England</td><td></td><td>✓</td></tr>
<tr><td>Gender</td><td>✓</td><td></td></tr>
<tr><td>Number of flowers in a garden</td><td></td><td>✓</td></tr>
</table>
2 marks for 4 correct ticks
1 mark for 2 or 3 correct ticks
0 marks for 0 or 1 tick
</td><td>2</td></tr>
</table>

Question	Answer	Marks
4(a)	Hacking	1
4(b)	Spyware	1
4(c)	Smishing	1

Question	Answer	Marks
5	Matched pairs from, for example: I always check whether wires are damaged/lose when I plug in my computer equipment ...This will reduce electrocution I always check whether sockets are safe/not broken when I plug in equipment... ...This will reduce electrocution I only plug in one plug per socket ...This reduces the chance of fire I make sure all wires are fastened to the wall/placed under carpets/in ducts//Use wireless... ...This reduces tripping hazards Check and install circuit breakers... ...This reduces electrocution/fire hazard Make sure no drinks or food is brought near to computers... ...This reduces electrocution I make sure computer vents are not covered... ...This reduces the chances of fire I make sure all IT equipment is safely in the middle of desks//I make sure strong tables are used to store IT equipment/I don't store IT equipment on high shelves... ...To stop them falling on me and causing an injury	6

Question	Answer	Marks
6	Max **four** from: Adds a level of security Verifies the email comes from a known and trusted source Provides the receiver with a means of reply/private key Used for initialising secure SSL connections between web browsers and web servers Max **three** from: Details of the owner of the digital certificate Serial number Public key Digital signature Subject name Valid from Valid to//Expiry date	**5**

Question	Answer	Marks
7	**Four** matched pairs: I never send personal data to people I do not know ... ... because people can use it against me … as other people can access my personal details I do not reply by using reply button unless I know the person ... ... because it may be a scam I use a list of known email addresses ... ... so I don't accidently send it to the wrong email address I check before opening an email/email attachment ... ... because it might be a phishing attack I scan both the email and attachment ... ... in order to avoid viruses I never send images of myself to people I do not know ... ... so they cannot recognise me in the street I do not set auto reply to my email system ... ... as this could alert a spammer that the email is active I use email filtering ... ... this stops spam emails I always report any phishing emails ... ... so the authorities can take action I change my email password regularly ... ... so that others cannot access my email account I use a strong password … … so that others cannot access my email account I logout of email after I have finished using it ... ... to stop others gaining access to my emails I keep my password safe … … so that others cannot access my account **To gain full marks at least three matched pairs are required**	8

Question	Answer	Marks
8a	**Two** from for example: Email address Real names DOB Home address Contact phone number Membership card number Location data Internet Protocol (IP) address Picture of yourself Gender	2
8b	**Two** from: Password should not relate to personal details Should be a long password Not previously used password Should not include repeating/obvious patterns//predictable words Password should be strong	3
8c	**Six** from: Use anti-spyware/up to date antivirus software Play the games with the firewall operational Play only with authorised versions of games which you have purchased from the correct sources and for which you have a licence Download/buy files and new software from reputable sources Do not forget to delete your account details when you are not playing again Keep the game software up to date. When disposing of your gaming device ensure all of your personal information has been deleted. Choose a username that does not reveal any personal information Be aware of criminals buying or selling 'property' that exists inside a computer game, in the real world	6

Question	Answer	Marks
9	**Six** from: Change default name/usernames and passwords on the router Change the default privacy//use a strong privacy setting Disable features not in use Use strong WiFi encryption Separate the IoT from the home WiFi account Keep software/hardware up to date Avoid public WiFi networks Ensure firewall is operational Use anti-spyware/up to date anti-virus Use strong passwords Use unique passwords for each device Change passwords regularly	6

Question	Answer	Marks
10a	**Two** from: Could be hardware or software Sits between the computer/network and the router Filters/controls/monitors data/traffic coming in and out of the college network **Four** from: Checks whether the data passing through it meets a given set of rules Blocks data that does not satisfy the rules Alerts user about unwanted data Can log all incoming and outgoing data/traffic to check later Can prevent/block access to undesirable/inappropriate websites/IP addresses Keeps a list of undesirable IP addresses Can prevent hackers gaining access to the system Can send out warnings Can block the unwanted traffic in and out of the network Keeps a list of desirable IP addresses/websites It can block IP addresses	6
10b	**Four** from: Anyone can post information on the internet Websites may contain incorrect information Any information found will need to be checked against reliable sources Similar websites may have conflicting data on the same topic The search engines tend to be generalised Search engines do not necessarily give the most reliable searches at the top of the list//paying to have information at the top of the list Data on the website could be out of date	4

Question	Answer	Marks
11a	**Four** from: Scrambling of data Changes the data into a form that is not understandable Requires a decryption key/encryption key to decode Encrypted using a encryption key/code Changes plain text into cypher text	4
11b	**Four** from: Use anti-spyware to prevent key logging Change passwords regularly//Do not repeat the same password Use a different password for each system Avoid common/predictable patterns as they are easier to guess Use longer passwords as they are harder to guess Use strong passwords Use two-factor authentication so that hackers need both parts Use a dropdown list for password entry Use a biometric password Do not use passwords that directly links to the user Do not allow webpages/device to remember the password	4

Question	Answer	Marks
12	Bank card Medical record	2

Question	Answer	Marks
13a(i)	**Fire** **Two** from: CO_2 fire extinguisher Don't overload sockets Have fans/cooling system Use Residual Circuit Breaker/RCB	2
13a(ii)	**Electrocution** Don't bring drinks close to computers Cover/insulate live/bare wires	2
13b	**Three** from: Report/block cyberbullies Respect other players Check game ratings for age Reduce the amount of time spent gaming Be careful of in-app purchases Turn on privacy settings Don't use your real name//use a nick name Don't give away personal information	3
13c	Max **two** from: Part of the authentication system Needed to improve security Max **three** from: Combined they are unique User ID is an identifier for the user Password is a string of characters Passwords verify the user in the authentication process	4

Question	Answer	Marks
14a	**Four** from: Data should be fairly and lawfully processed//Data should be processed in a transparent manner Data should only be processed for the stated purpose Data should be adequate, relevant and not excessive/limited Data should not be kept longer than necessary Data should be processed in accordance with the data subject's rights Data should be collected for specific purposes Data should only be further processed for archive purposes which is compatible with the initial purposes Data kept for archiving should safeguard the rights and freedoms of individuals Explicit consent required for processing sensitive data Data subjects are allowed access to their personal data Data should be accurate and kept up to date Data should not be transferred to another country unless they have adequate protection Parental consent required for processing personal data of children including online services	4

14b	**One** mark for the explanation Personal data is data relating to an individual/person that can be identified **One** mark per example Name, address, date of birth, gender, biometrics, mobile/cell phone number, credit/debit card number, personnel ID number, personal appearance, medical record, criminal record, ethnic origin, picture of yourself, political opinions, religious or philosophical beliefs, trade-union membership record, genetic data, IP address, racial identity	3
14c	**Four** from: The person can be identified from the data The data is confidential as it links directly to the person If someone gets access to the data then they can use the information to attack the person If not kept confidential and secure it could lead to home burglaries as people post holiday details on social media If not kept confidential and secure it could lead to the chance of users suffering physical harm Protects sensitive data	4

Question	Answer	Marks
15a	**Three** from: Automatic backup More storage Difficult to lose the data as many copies are made of it Many people can share access to the data Can be accessed anywhere there is internet connection Can be accessed from many devices	3
15b	**Three** from: No control over data/security Requires internet access If the company goes out of business can lose data If the internet crashes during sending or receiving then data could be lost Many copies are made of the data which increases security issues More expensive in the long run due to monthly charges	3

Question	Answer	Marks
16a	**Four** from: Be careful of impersonators/people pretending to be officials Safely dispose of personal information Encrypt your data Keep passwords private/Use a strong password Don't share personal data Keep privacy settings high Use security software/anti-spyware Avoid phishing emails Use a nickname/alias online	6

16b	**Four** from: **For policed** Prevents illegal material being readily available Prevents young children accessing unsuitable material Ensures copyright laws are maintained Stops extreme viewpoints from being seen Prevents libelous text being added Prevents hate comments/foul language/racial comments **Against policed** Governments block text/viewpoints/their own bias viewpoint Unsuitable material is easily available in other ways Control would cost money and users would have to pay Control would be very difficult to enforce Could cause less people to use it Laws are different in each country but the internet is world wide Creates a feeling of big brother/always being watched **To gain full marks the discussion must have correct answers for both for and against policed**	4

Question	Answer	Marks
17a	**Eight** from: **For** Face can be identified faster Face can be identified by electronic comparison therefore relative higher level of accuracy Facial recognition can uniquely identify individuals Can automatically compare faces from older images System can work continuously but a human checker would need to take breaks **Against** Dark glasses/facial hair/face coverings may cause the facial recognition systems to not work More difficult to change biometric data Recognising a person can be slower as more checking is carried out Harder to set up the facial recognition system Takes longer to add new people to the system Biometrics can use a lot of memory to store the data Intrusive as personal details have to be stored More likely to be affected by the environment With the video system each frame needs to be checked with known images which can lead to errors **To gain full marks the discussion must have correct answers for both for and against**	8

17b	**Three** from: Finger print Hand print Vein geometry Retina Iris Speech/Voice	3

Question	Answer	Marks
18	**Six** from: I block unwanted messages/suspicious users… …and report the sender Before using the messaging system, I check how to block and report unwanted users… …this stops predators I never arrange to meet strangers alone I always tell a responsible adult if I plan to meet someone I always meet in a public place I avoid giving away personal information I report abusive messages from a sender of the messages I report cyber-bullying When sending messages I always use appropriate language If someone messages me with private and personal information about themselves I respect their confidentiality/privacy I always read carefully the messages before I send I avoid sarcasm I am not offensive when replying I carefully check that I am replying to the correct person I do not enable my location when messaging	6

Question	Answer	Marks
19	**Six** from: The data will have the name/medical information attached therefore it needs protecting The data is confidential as it links directly to the person The data will be sensitive To prevent blackmail/bullying from using medical results To prevent fraud from using financial information To prevent identity theft using contact details To avoid the doctor's surgery getting fined if it got made public The doctor's surgery's reputation would suffer Patients would lose trust	6

Question	Answer	Marks
20	**Eight** from: **Benefits** Faster way of accessing systems Cannot forget the biometric data Must be physically at the device to access it More secure as it uses unique data Difficult to copy/forge **Drawbacks** Invasion of privacy User may not know they have logged off Biometrics may change therefore data will need to be kept up to date Expensive method/technology to set up Environment can affect measurements Over usage can affect the measurements Difficult to reset once compromised Difficult to set up Time consuming to set up as measurements must be taken Facial coverings/changes can prevent system from working **To gain full marks the discussion must have correct answers for both benefits and drawbacks**	8

Question	Answer	Marks
21a	**Six** from: • User IDs and passwords combined protect against unauthorised access Combined user ID and password is unique to the computer system. • The user ID ensures the correct account is accessed, the password then protects the account • If someone knew the user ID they could only gain access with the correct password • Typing in incorrect user ID/password a number of times could lock the user out • User IDs give different access levels in the computer system • User IDs are unique and allow the system manager to monitor usage on the system • The password is masked and displayed as stars • A strong password is a combination of upper and lower case characters/numbers/symbols • Passwords could be biometrics ensuring greater security • Passwords increase security as they are only known by the user	6

21b	**Description** **Two** from: • Uses parts of the body/physical attributes as a password • Unique to the user • Form of authentication **Examples** **Two** from, for example: • Fingerprint • Retina • Voice • Face	4

Question	Answer	Marks
22a	**Two** from: It's a fraudulent practice of making phone calls/leaving voice messages The caller pretends to be from a reputable company Forces individuals to reveal personal information Voice mail/VOIP/phone call phishing	2
22b	**Two** from: Never give out personal information to the caller Ring the bank/company on a known number Hang up and do your own investigation Block their number Don't answer the call if you do not recognise the number	2

Question	Answer	Marks
23a	Encryption	1
23b	Control	1
23c	Hacking	1
23d	(An) interview	1

Question	Answer	Marks
24a	Password: 6lRrg08& **Two** from: No obvious sequence of numbers/letters Long password Strong password Hard to guess Not directly related to personal details	3
24b	**One** from: Changing password regularly Use of anti-spyware/anti-malware Be aware of shoulder surfing	1

Question	Answer	Marks
25	**Four** from: Block and report unwanted users Do not meet an online contact face to face Always tell an adult if you plan to meet in person Avoiding the distribution of inappropriate images when sending to new friends Avoiding the use of inappropriate language Respecting confidentiality/personal/sensitive data of new friends Never reveal personal images Keep personal data private Set account privacy settings Turn off current location	4

Question	Answer	Marks
26a	**Three** from: A type of credit card theft A digital copy of the credit card is made with data placed on a new blank card An unauthorised copy is made of the data Uses a concealed electronic scanner	3
26b	**Two** from: Use of personal identification number/PIN Use of chipped cards Inspect the credit card reader you are using Use an RFID protector Sign up for text alerts on the account Not using your credit card if you feel unsafe/suspicious websites Don't let your card leave your sight Use third party/smartphone electronic payment systems	2

Question	Answer	Marks
27a	Visual verification	1
27b	**Four** from: Data is processed lawfully/fairly Data processing must be transparent The purpose of collecting the data must be specified/explicit/legitimate Personal data must be adequate/relevant/not excessive Personal data must be accurate/kept up to date Personal data must not be kept for longer than is necessary Personal data must be processed in a secure manner Data can only be used for medical purposes Data must be protected	4

Question	Answer	Marks
28a	**Two** from: It is a security method Form of security to protect the resources/data that the user can access Adds another layer of security	2
28b	**Two** from: Security token Biometrics GPS signal Receive/send a code you have to enter by email/SMS Username and Password Credit card number Phone number/email address Dongle/security app	2

Question	Answer	Marks
29a	**Two** from: Watching/spying on the user entering the password/data Watching/spying on the user to memorise the data/password People can eavesdrop/listen when personal data is being exchanged	2
29b	**Two** from: Cover the key pad when entering the password When entering your password in a public place, sit with your back to the wall//Enter password when no one is nearby Unclick show password Use biometrics Use contactless cards	2

Question	Answer	Marks
30a	**Two** from: Keylogging is a software/hardware device It records/sends to a third party every keystroke on your keyboard It can gain fraudulent access to passwords/confidential information.	2
30b	**Two** from: Install anti-keylogging/anti-malware/anti-spyware software Check the computer system before entering confidential data Update the computer system regularly	2

Question	Answer	Marks
31(i)	**Three** from: Protects the computer against computer viruses The AV has a database of known viruses Identifies a virus with those stored in its database Prevents malicious script from running Alerts the user that a virus is found It is a security method Removes/quarantines viruses	3
31(ii)	**Three** from: Protects against malware/malicious software Detects more advanced forms of malware Uses heuristic-based detection Finds source codes that indicate a threat It is a security method Warns of the threat if it identifies malware Contains a database of code Removes the malware	3

32	**Six** from: Strong passwords make it harder to crack the password Change passwords frequently using an unused password Change passwords regularly to ensure that unauthorised access is lower Use different passwords on different accounts to ensure that if one password is guessed others are safe Using biometric passwords as these are unique to the user Biometric passwords are very hard to forge Safer to use a combination of different types of password For added security a One Time Password could be used Ensure that the password cannot be linked back to the user as it makes it easier to guess Biometric passwords can be affected by the environment Biometric passwords can be affected by human changes OTP / biometric passwords require extra hardware to be used	6