SUPERNOVA SCHOOL (SNS)

CAMBRIDGE COMPUTING — GRADE 6

UNIT 3: NETWORKS & DIGITAL COMMUNICATION

Worksheet Answer Key: Topics 3.1 and 3.2

SECTION A: STORING AND TRANSFERRING DATA ON A NETWORK

Question 1: Complete the Sentences

1. Digital communication
2. Animations
3. Server
4. Intranet
5. Streaming
6. Wired
7. Radio
8. Bandwidth
9. Router
10. Cellular
11. GPS (Global Positioning System)
12. Network overload

Note: Other suitable answers may be accepted where appropriate.

Question 2: Answer the Following Questions

a. What is digital communication? Give two examples.

Digital communication is the electronic exchange of information between devices.

Examples:

- Sending an email.
- Making a video call.

b. What is digital content? Name four types.

Digital content is information that can be stored or transmitted digitally.

Examples include text, images, audio, and video.

c. Explain the role of a server in a computer network.

A server is a computer that stores and manages data and provides resources or services to other devices on a network.

d. What is an intranet? Give one school example.

An intranet is a private network used within an organisation. A school might use an intranet to share lesson plans, announcements, and learning resources with staff.

e. Explain the difference between downloading a file and streaming a video.

Downloading transfers a file to a device so that it can be stored and accessed later. Streaming sends data continuously or in small parts, allowing a video or audio file to play before the entire file has arrived.

f. Give two advantages of streaming.

1. Users can start watching or listening without waiting for the entire file to download.
2. Streaming can reduce the need to store large media files permanently on a device.

g. State two differences between wired and wireless networks.

Wired Network	Wireless Network
Uses physical cables to connect devices.	Uses radio waves to connect devices.
Usually provides a stable connection with low interference.	Allows greater mobility but may experience wireless interference.

h. Explain how Wi-Fi allows a device to connect to a network.

Wi-Fi uses radio waves to connect a device wirelessly to a local network, usually through a wireless access point or router.

i. Describe the purpose of a router.

A router directs data between networks and can share an internet connection among multiple devices.

j. Explain how a cellular network allows people to access the internet while travelling.

A cellular network uses mobile communication towers to connect a phone to the network. As the person travels, the phone can connect to different towers, allowing mobile data services to continue where coverage is available.

Question 3: Identify the Correct Networking Term

1. Server
2. Streaming
3. Wired network
4. Wireless network
5. Intranet
6. Cellular network
7. GPS
8. Network overload

Question 4: True or False?

1. **True**
2. **True**
3. **False** — Streaming allows playback to begin before the entire video has been received.
4. **True**
5. **True**
6. **False** — GPS helps determine location using satellites, while cellular networks provide mobile communication and data services.
7. **True**
8. **True**
9. **True**
10. **False** — More connected devices can increase network demand and may slow the connection.

SECTION B: BANDWIDTH AND NETWORK OVERLOAD

Question 5: Understanding Bandwidth

a. Define bandwidth.

Bandwidth is the maximum amount of data that can be transmitted over a network connection in a given amount of time.

b. Explain the relationship between bandwidth and data transmission.

Higher bandwidth allows more data to be transmitted in the same amount of time. Lower bandwidth limits the amount of data that can be transmitted.

c. Give two possible reasons for a video repeatedly pausing.

1. The available bandwidth may be too low.
2. Too many devices may be using the network at the same time.

d. Why may higher bandwidth improve streaming?

Higher bandwidth allows more data to be transmitted at a time, helping videos load more smoothly when sufficient capacity is available.

e. Explain the road comparison.

A road with more lanes can carry more traffic at once. Similarly, a network with higher bandwidth can carry more data in a given amount of time.

Question 6: Scenario — The Busy School Network

a. Identify the network problem.

Network overload or network congestion.

b. Explain why the network has become slow.

Many students and teachers are downloading large files and streaming videos simultaneously. Their combined demand may exceed the available network bandwidth.

c. Give two symptoms of network overload.

1. Videos pause or buffer repeatedly.
2. Websites and files take longer to load or download.

d. Suggest three ways to reduce network congestion.

1. Pause downloads that are not currently needed.
2. Schedule large downloads outside busy school hours.
3. Limit unnecessary high-bandwidth activities during lessons.

e. Why could increasing bandwidth help?

It would increase the amount of data the network can transmit in a given amount of time, helping it handle more simultaneous activities.

f. Would increasing bandwidth guarantee that overload could never occur?

No. Network overload could still occur if demand becomes greater than the available capacity. Other network limitations can also affect performance.

Question 7: Apply Your Knowledge

1. **A — Wired Ethernet connection**

2. **B — Wi-Fi**
3. **A — The available bandwidth may become insufficient for all activities.**
4. **C — Pausing downloads that are not currently needed**
5. **B — GPS**

SECTION C: NETWORK CONNECTIONS IN REAL-LIFE SITUATIONS

Question 8: Wired or Wireless?

Scenario 1: School computer laboratory

Connection: Wired

Reason: A wired connection generally provides a stable and reliable connection for programming tasks.

Scenario 2: Tablet in the school library

Connection: Wireless

Reason: Wi-Fi allows the student to connect without using a physical network cable.

Scenario 3: Office computers transferring large files

Connection: Wired

Reason: Ethernet connections generally provide stable, reliable data transfer and are less affected by radio interference.

Scenario 4: Smartphone at a café

Connection: Wireless

Reason: Wi-Fi allows the visitor to access the internet without connecting the phone to a cable.

Scenario 5: Hospital desktop computers

Connection: Wired

Reason: A wired network can provide a stable and reliable connection for accessing important patient records. Appropriate security measures are also required.

Scenario 6: Internet access on a bus

Connection: Wireless

Reason: A cellular network allows the person to access mobile data while travelling, provided mobile coverage is available.

Accept other suitable answers if students provide a reasonable explanation.

SECTION D: SECURING DATA

Question 9: Complete the Sentences

1. Data security
2. Authentication
3. Password
4. Fingerprint
5. Facial
6. Phishing
7. Theft
8. Encryption
9. Phishing
10. Strong

For Question 1, accept "securing data" or "data security." For Question 6, "phishing" is the expected answer.

Question 10: Why Must Data Be Kept Secure?

a. Why does personal data need protection?

Personal data needs protection because unauthorised people could steal, misuse, or share it without permission. This could lead to fraud, identity theft, or loss of privacy.

b. Give three examples of sensitive information.

1. Home address and date of birth.
2. Bank account details.
3. Medical records.

c. What is unauthorised access?

Unauthorised access occurs when someone accesses a device, account, or data without permission.

d. Give two problems caused by stolen personal information.

1. Someone could use the information to pretend to be another person.
2. Someone could use it to commit fraud or access private accounts.

e. Explain the difference between fraud and identity theft.

Fraud involves deceiving someone to gain an unfair or illegal benefit, often money. Identity theft occurs when someone uses another person's personal information to pretend to be that person.

f. Why should login details remain private?

Keeping login details private reduces the risk of unauthorised people accessing accounts, viewing personal information, or changing or deleting data.

Question 11: User Authentication

a. What is user authentication?

User authentication is the process of checking that a user is who they claim to be before allowing access to a device, system, or account.

b. State three authentication methods.

1. Password
2. Fingerprint recognition
3. Facial recognition

A PIN or security key is also acceptable.

c. How does fingerprint recognition work?

A fingerprint sensor scans the user's fingerprint and compares it with the stored reference data. If the system finds a sufficient match, it allows access.

d. Give one advantage and one limitation of facial recognition.

Advantage: It allows a user to unlock a device without typing a password.

Limitation: It may fail to recognise the user under certain conditions, or its reliability may depend on the device and system being used.

e. Why should a password be difficult to guess?

A difficult-to-guess password makes it harder for unauthorised people to access an account.

f. Why is reusing the same password risky?

If one account is compromised, someone may try the same password on the user's other accounts, putting them at risk.

g. Is a username and password alone two-factor authentication?

No. A password is one authentication factor. A username identifies the account but is not a second authentication factor. Two-factor authentication requires two different types of evidence, such as a password and a fingerprint.

Question 12: Evaluate Password Strength

Suggested ratings are provided below. Ratings may vary slightly if students justify their choices appropriately.

Password	Suggested rating (1–5)	Reason
Arun123	1	Short and predictable; contains a name and a common number sequence.
qwerty123	1	Uses a common keyboard pattern and predictable numbers.
Purple123	1	Contains a common word followed by predictable numbers.
CatLoverP@ncake!492	4	Long and contains uppercase and lowercase letters, symbols, and numbers, although its words may be predictable.
Pomegranate23	2	Longer than some examples but uses a dictionary word followed by predictable numbers.

a. Which password is strongest?

CatLoverP@ncake!492 is the strongest option in this list because it is relatively long and includes different character types. However, it is not guaranteed to be secure, particularly if its words or pattern are predictable.

b. Which password is weakest? Give two reasons.

qwerty123 is one of the weakest because:

1. It uses a common keyboard pattern.
2. It ends with a predictable number sequence.

c. State three characteristics of a strong password.

1. It is long, preferably at least 12 characters.
2. It is difficult to guess and does not contain easily guessed personal information.
3. It avoids common patterns and reused passwords.

d. Why might a long password made from predictable words be vulnerable?

Attackers can use tools that test common words and predictable combinations. Length helps, but predictability can make a password easier to guess.

e. Suggest three ways to improve a weak password.

1. Replace predictable patterns with a less predictable combination.
2. Make the password longer.
3. Use a randomly generated password or a long, unique passphrase.

f. Why should passwords avoid personal information?

Names, birthdays, and other personal details may be easy to discover or guess, making passwords based on them less secure.

g. Create a strong password and explain two features.

Example: River!Cloud7Maple#42

Features:

1. It is long and contains uppercase and lowercase letters, numbers, and symbols.
2. It does not directly use a person's name or birthday.

This is an illustrative example. Students should not adopt a password displayed in a shared worksheet as their actual password.

SECTION E: RECOGNISING ONLINE SECURITY RISKS

Question 13: Safe or At Risk?

Scenario 1: Email claiming to be from a bank

Decision: At Risk

Reason: The email may be a phishing attempt. Ali should not click the link or enter his password. He should contact the bank through an official channel if verification is needed.

Scenario 2: Sharing personal details publicly

Decision: At Risk

Reason: Strangers could misuse Sara's address, phone number, or date of birth.

Scenario 3: Using different strong passwords

Decision: Safe

Reason: Different strong passwords reduce the risk that one compromised password will put multiple accounts at risk.

Scenario 4: Message offering a free laptop

Decision: At Risk

Reason: The message may be a scam designed to steal Ayesha's bank details. She should not provide the information.

Scenario 5: Opening an unknown attachment

Decision: At Risk

Reason: The attachment could contain malware or lead to a harmful website. Usman should verify the sender and check the attachment before opening it.

Scenario 6: Visiting the official bank website independently

Decision: Safe

Reason: Mariam avoids the suspicious link and independently accesses the bank's official website. She should still verify the address carefully.

Question 14: Understanding Phishing

a. What is phishing?

Phishing is a type of online scam in which an attacker pretends to be a trusted person or organisation to trick someone into revealing information or performing an unsafe action.

b. Describe three ways phishing can occur.

1. **Email phishing:** A fake email asks the user to click a link or provide login details.
2. **Text-message phishing:** A fraudulent text contains a harmful link or requests personal information.
3. **Phone-call phishing:** A caller pretends to represent a trusted organisation to obtain private information.

Other acceptable answers include phishing through social media messages or fake websites.

c. Why might a phishing message appear trustworthy?

The sender may imitate a real organisation's name, logo, writing style, or email address to make the message appear genuine.

d. Give three warning signs of phishing.

1. Unexpected requests for passwords or financial information.

2. Suspicious links or website addresses.
3. Messages that create urgency or promise unexpected prizes.

e. What should you do if a suspicious message asks for your password?

Do not click its links or share the password. Report the message, delete it if appropriate, and verify the request through an official channel.

f. Why is a padlock symbol not enough to prove a website is trustworthy?

The padlock indicates that the connection is encrypted, but it does not guarantee that the website itself is genuine. A fraudulent website can also use an encrypted connection. Users should check the website address and confirm that the site is legitimate.

SECTION F: EXTENDED SCENARIO-BASED QUESTIONS

Question 15: The School Network

a. Identify the device that stores the school's shared learning materials.

The server.

b. Give one benefit of a central server.

It allows authorised users to access shared learning materials from different computers without keeping separate copies on every device.

c. Which connection is most suitable for laboratory desktop computers?

A wired Ethernet connection is generally suitable because it provides a stable and reliable connection.

d. How does wireless connectivity benefit teachers?

It allows teachers to connect laptops and tablets to the school network without being physically connected by network cables, making movement easier.

e. Explain how bandwidth and network overload may cause slow performance.

Bandwidth determines how much data can be transmitted in a given amount of time. If many students stream videos or download files simultaneously, their combined demand may exceed the available capacity. This can cause buffering and slow website loading.

f. Suggest two ways to improve performance.

1. Increase the available network bandwidth if the existing connection is insufficient.

2. Schedule large downloads outside busy periods or reduce unnecessary high-bandwidth activities.

g. Why should access to the server and shared files be protected?

The school needs to prevent unauthorised people from viewing, stealing, changing, or deleting important information.

h. Recommend two security measures.

1. Use strong, unique passwords and appropriate user authentication.
2. Apply suitable access permissions so users can only access the files they are authorised to use.

Other suitable measures include encryption, security updates, and reliable backups.

Question 16: Protecting an Online Account

a. Identify the possible security threat.

Phishing.

b. Give two warning signs.

1. Zara does not recognise the sender.
2. The email unexpectedly asks her to confirm account details through a link.

c. What should Zara do instead of clicking the link?

She should avoid clicking the link and access the learning platform through its official website or app. If necessary, she should contact the school or platform administrator through a trusted channel.

d. Why is reusing passwords risky?

If one account is compromised, an attacker may try the same password on Zara's other accounts.

e. Recommend two ways to improve account security.

1. Use a different, strong password for each account.
2. Enable multi-factor authentication where available.

f. How does authentication protect Zara's schoolwork?

Authentication checks a user's identity before allowing access, helping prevent unauthorised people from viewing or changing her schoolwork.

g. How can fingerprint authentication help?

The device compares Zara's fingerprint with stored reference data. If it matches sufficiently, the device allows access, reducing reliance on a password alone.

SECTION G: CHALLENGE QUESTIONS

Question 17: Choose and Justify

a. Why might the internet connection become slow?

Many devices are streaming videos and downloading a large file at the same time. The combined demand may exceed the available bandwidth.

b. Identify one activity that could be paused.

The large file download could be paused until the network is less busy.

c. Why could increasing bandwidth help?

It would increase the amount of data that can be transmitted in a given amount of time, allowing the network to handle more simultaneous activities.

d. Suggest one additional way to improve performance.

Schedule large downloads for quieter periods or stop unnecessary streaming activities.

Question 18: Explain the Differences

a. Server and router

A server stores and manages data or provides services to other devices. A router directs data between networks and can share an internet connection.

b. Wired and wireless networks

A wired network connects devices using physical cables. A wireless network uses radio waves to connect devices without physical network cables.

c. Streaming and downloading

Streaming allows content to play while data is being received. Downloading transfers a file to a device for storage and later access.

d. Bandwidth and network overload

Bandwidth is the maximum amount of data that can be transmitted over a connection in a given amount of time. Network overload occurs when demand on the network exceeds its available capacity.

e. Authentication and encryption

Authentication checks whether a user is who they claim to be. Encryption changes readable data into a protected form so that unauthorised people cannot easily understand it.

f. Phishing and identity theft

Phishing is an attempt to trick someone into revealing information or performing an unsafe action. Identity theft occurs when someone uses another person's personal information to pretend to be them.

Question 19: A Complete Network and Security Plan

Sample Answer

A school can use a server to store digital textbooks, videos, assignments, and research materials. This allows authorised students and teachers to access shared resources.

Wired Ethernet connections can be used for desktop computers because they generally provide stable and reliable connections. Wi-Fi can be provided for laptops and tablets so that students and teachers can connect without network cables.

The school should ensure that sufficient bandwidth is available to support its users. If too many students stream videos or download large files at the same time, network overload may occur. The school can reduce congestion by scheduling large downloads outside busy hours and upgrading the network connection if necessary.

Student data must be protected from unauthorised access. The school should use strong passwords, appropriate user authentication, and access permissions. Encryption can also help protect sensitive information.

Phishing is one possible online security threat. Students should avoid suspicious links, never share passwords through unexpected messages, and access learning platforms through official websites or apps.

These measures can help the school maintain an efficient network while protecting student information.

TEACHER'S MARKING NOTES

- Accept alternative answers when they demonstrate correct computing knowledge.
- Award credit for appropriate examples and clear explanations.
- In scenario-based questions, accept different connection choices when the student provides a technically sound justification.

- In password questions, treat the numerical ratings as suggested judgements rather than absolute security measurements.
- In Question 19, assess whether students explain the key concepts and apply them appropriately to the school scenario.
- For security questions, distinguish between **authentication** (verifying identity), **encryption** (protecting the meaning of data), and **phishing** (tricking users into disclosing information or taking unsafe actions).

End of Answer Key