Grade 8 Pre-Technical Studies

Terms 1, 2 and 3 - notes for 14 topics

IN EVERY TOPIC

- What you will learn and the key words.
- Short, clear notes with worked examples.
- Questions to try and a topic test, with the answers at the back.

TOPICS IN THESE NOTES

Topic	Name	Term
1.1	Fire Safety	1
1.2	Data Safety	1
2.1	Plane Geometry	1
2.2	Dimensioning	1
2.3	Plain scale drawing	1
2.4	Visual programming	2
3.1	Composite Materials	2
3.2	Ceramics	2
4.1	Cutting Tools	2
4.2	Computer Software	3
5.1	Bookkeeping	3
5.2	Income and Budgeting	3
5.3	Marketing goods and Services	3
5.4	Distribution of Goods and Services	3

Elimu254 • Learn • Grow • Build Tomorrow

CONTENTS

Topic	Name	Term	Page
1.1	Fire Safety	1	3
1.2	Data Safety	1	6
2.1	Plane Geometry	1	10
2.2	Dimensioning	1	12
2.3	Plain scale drawing	1	16
2.4	Visual programming	2	18
3.1	Composite Materials	2	22
3.2	Ceramics	2	25
4.1	Cutting Tools	2	28
4.2	Computer Software	3	33
5.1	Bookkeeping	3	36
5.2	Income and Budgeting	3	40
5.3	Marketing goods and Services	3	43
5.4	Distribution of Goods and Services	3	46
	Answers		49

Elimu254
Learn • Grow • Build Tomorrow

Strand 1.0 Foundations of Pre-Technical Studies | Term 1

1.1 Fire Safety

WHAT YOU WILL LEARN

By the end of this topic you should be able to:

- identify possible causes of fire outbreaks in the environment
- explain ways of preventing fire outbreaks in the environment
- extinguish fires in the environment using appropriate methods
- acknowledge the need for fire safety in day-to-day life

KEY WORDS

fire, combustion, flammable, combustible, electrical fault, cooling, smothering, starving, interrupting, extinguisher.

1. Meaning and importance of fire

Useful but dangerous

Fire is the heat and light given out when a fuel burns quickly in oxygen (combustion).

Uses at work: cooking in hotels and schools; welding and metal work in jua kali workshops; firing pottery and bricks; heating; generating electricity.

Out of control, fire destroys life, property and the environment; fire safety prevents this.

2. Causes of fire outbreaks

Causes

Flammable substances: petrol, paraffin, cooking gas, thinners and spirit catching fire from flames or sparks; leaking gas cylinders.

Electrical faults: overloaded sockets, damaged cables, poor or illegal connections, faulty appliances left on.

Combustible materials: paper, wood shavings, cloth and rubbish piled near heat sources.

Human carelessness: smoking, unattended candles and jikos, children playing with matches, arson.

3. Preventing fire outbreaks

Prevention

Store flammable liquids in labelled, closed containers away from heat; no smoking or open flames near them.

Use qualified electricians; do not overload sockets; switch off and unplug equipment after use; replace damaged cables.

Keep the workshop tidy: sweep up shavings and rubbish daily; keep exits clear.

Never leave flames unattended; keep fire extinguishers, sand and fire blankets ready and serviced; post fire rules and emergency numbers (999, 112).

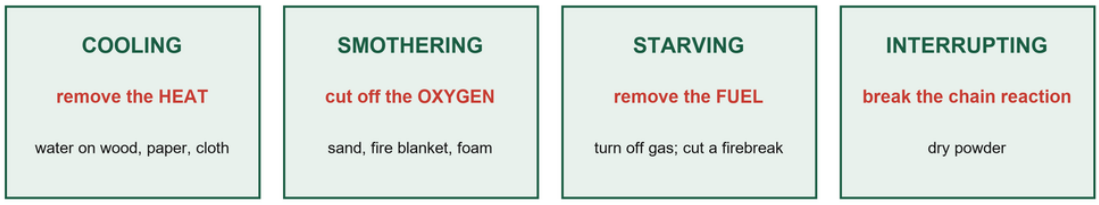
4. Firefighting techniques: cooling and smothering

Removing heat or oxygen

A fire needs fuel, heat and oxygen (the fire triangle) and a chain reaction between them (the fire tetrahedron).

Cooling: removing heat, usually with water, for burning wood, paper and cloth. Never use water on oil, petrol or electrical fires.

Smothering: cutting off oxygen with sand, soil, a fire blanket, foam or carbon dioxide; suits small fires, burning pans of oil and fuel spills.



Four firefighting techniques

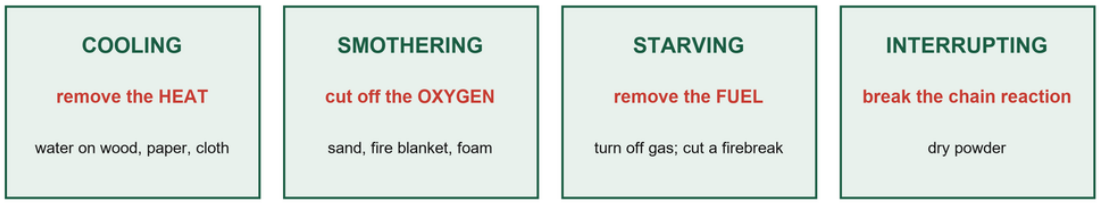
5. Firefighting techniques: starving and interrupting

Removing fuel or breaking the chain

Starving: removing the fuel; turning off a gas or fuel supply; moving combustible materials away; cutting a firebreak in grass.

Interrupting the chemical chain reaction: some extinguishing agents (dry powder, certain special agents) stop the reaction between fuel, heat and oxygen.

Match: burning grass, starve with a firebreak; leaking gas fire, turn off the supply and use dry powder; burning paper bin, cool with water; oil pan, smother.



Four firefighting techniques

6. Role-playing firefighting

Practical: role play

Materials: training extinguisher or mime, fire blanket or damp cloth, sand bucket, whistle.

First raise the alarm, switch off power if safe, and make sure your exit is clear.

Extinguisher: PASS: Pull the pin, Aim at the base, Squeeze the handle, Sweep side to side.

Groups act scenarios: a smouldering bin (cool), a burning pan (smother), a spreading grass fire (starve and evacuate).

Finish with an evacuation drill to the assembly point.

7. Fire safety in day-to-day life

Summary

Causes: flammable substances, electrical faults, combustible materials, carelessness.

Prevention: safe storage, safe wiring, tidiness, never leaving flames, ready equipment.

Firefighting: cooling, smothering, starving, interrupting; PASS for extinguishers; evacuate if unsafe.

Each learner checks one fire risk at home and suggests a fix.

TRY THESE

1. What is fire?
2. Give three uses of fire at work.
3. Name three flammable substances.
4. Give two electrical causes of fire.
5. Give three ways of preventing fires in a workshop.
6. Why keep exits clear?
7. What does cooling remove?
8. What does smothering remove?
9. What does starving remove?
10. Give an example of starving a fire.
11. What does PASS stand for?
12. Where is an extinguisher aimed?
13. Name three causes of fire.
14. Name the four firefighting techniques.

TOPIC TEST

T1. Why do welders wear protective clothing?
T2. Why are wood shavings in a workshop a fire risk?
T3. Design a fire safety poster for the school workshop.
T4. Which technique would you use on a burning frying pan? Why?
T5. Why is dry powder useful for many classes of fire?
T6. Write a short fire procedure for your workshop.
T7. Draw a fire escape plan for your home.

Elimu254
Learn • Grow • Build Tomorrow

Strand 1.0 Foundations of Pre-Technical Studies | Term 1

1.2 Data Safety

WHAT YOU WILL LEARN

By the end of this topic you should be able to:

- outline the importance of data in an electronic device
- identify threats to data in an electronic device
- describe ways of protecting data in an electronic device
- secure data in an electronic device
- acknowledge the need for data safety in day-to-day life

KEY WORDS

data, information, electronic device, virus, malware, unauthorised access, password, antivirus, backup, update.

1. Data and information

Raw facts and meaning

Data is raw facts and figures (numbers, words, pictures, sounds) without context, for example 45, 52, 61.
Information is processed data that has meaning, for example "Wanjiru's maths scores rose from 45 to 61 this year."
Electronic devices storing data: phones, computers, tablets, smart cards, flash disks, cameras.
Examples: contacts, photos, messages, school reports, business records, mobile money records.

2. Importance of data

Why data matters

Data helps people and organisations make decisions, keep records (sales, health, school results), communicate, plan, and prove transactions.
Effects of losing data: lost records and money, inability to work, broken trust, privacy harm if data is stolen, costly recovery.
Personal data (names, phone numbers, ID numbers, photos) is protected by Kenya's Data Protection Act (2019).

3. Threats: viruses and malware

Harmful programs

A computer virus is a harmful program that copies itself and spreads, damaging or deleting data. Malware is any harmful software (viruses, worms, spyware, ransomware).
How they spread: infected flash disks; downloads from untrusted websites; email attachments and links from strangers; pirated software and games.
Signs: slow device, strange pop-ups, missing or changed files, programs crashing.

4. Threats: unauthorised access

Getting in without permission

Unauthorised access is when someone uses a device, account or data without permission.
How it happens: weak or shared passwords; devices left unlocked; shoulder surfing (watching you type); phishing messages tricking people into giving passwords or codes; hacking.
Effects: stolen money (for example through mobile money), privacy loss, impersonation, bullying.
Other threats to data: physical damage (water, falls), theft of devices, power failure while saving.

5. Protecting data with strong passwords

Practical: password strength

Materials: paper, school device.

A strong password is long (at least 8 to 12 characters), mixes capital and small letters, numbers and symbols, and is not easy to guess (not your name, birthday or "1234").

A passphrase is easier to remember: for example "Mangoes!Grow3Tall" (practice example only).

Rules: never share it; use different passwords for different accounts; change it if you think it is known.

Practise judging made-up passwords as weak or strong.

6. Screen locks and access control

Practical: locking a device

Materials: school device.

Set a screen lock: PIN, pattern, password or fingerprint.

Set the screen to lock automatically after a short time.

Log out of shared computers; use separate user accounts; do not let strangers use your device.

Teacher demonstrates on a school device; learners practise the steps on school devices.

7. Antivirus software

Practical: scanning

Materials: school computer with antivirus, flash disk.

Antivirus software detects, blocks and removes viruses and other malware.

Steps: open the antivirus program; choose a quick or full scan; scan the computer and any flash disk before opening its files; quarantine or delete threats found.

Keep antivirus and the operating system updated, because new threats appear daily.

8. Backing up data

Practical: backup

Materials: school computer, sample files, flash disk or cloud folder.

A backup is a copy of data stored somewhere else so it can be restored if the original is lost.

Methods: copy to a flash disk or external drive; save to cloud storage; back up phone contacts and photos.

Back up regularly; keep the backup in a different place from the device.

Practise: copy sample files to a backup folder, then "restore" one.

9. Safe online habits

Think before you click

Do not open links or attachments from strangers; check the sender.

Never share PINs, passwords or one-time codes, even with people claiming to be from a bank or school.

Download apps only from official stores; check app permissions.

Think before posting personal information or photos.

Sort made-up messages into "safe" and "suspicious".

10. Securing data: practical review

Practical: security checklist

Materials: school computers.

In groups, check a school computer: Is there a password? Is the screen lock on? Is antivirus installed and updated? Are files backed up? Are there unknown programs?

Fix what can be fixed under supervision and record findings and actions.

Report anything serious to the ICT teacher.

11. Data safety in day-to-day life

Summary

Data is valuable; losing or exposing it costs money, privacy and trust.

Threats: viruses and malware, unauthorised access, physical damage and theft.

Protection: strong passwords, screen locks, antivirus scans, updates, backups and safe online habits.

Each learner writes three data safety rules they will follow.

TRY THESE

1. What is data?
2. What is information?
3. Give three uses of data.
4. Give two effects of losing data.
5. What is a computer virus?
6. Name three ways viruses spread.
7. Define unauthorised access.
8. Give three ways it happens.
9. Give three features of a strong password.
10. Weak or strong: "kamau2010"?
11. Name three types of screen lock.
12. Why set an automatic lock?
13. What does antivirus software do?
14. When should a flash disk be scanned?
15. What is a backup?
16. Name two backup methods.
17. Give three safe online habits.
18. What should you do with a "you have won" message asking for a fee?
19. Name four items on the security checklist.
20. What did your group find?
21. Name two threats to data.
22. Name four ways to protect data.

TOPIC TEST

T1. Is a list of marks without names data or information?

T2. Why do hospitals need to protect patients' data?

T3. Why is pirated software risky?

T4. Why do banks never ask for your PIN by phone?

T5. Why is a long passphrase hard to guess?

T6. What is two-step verification?

T7. Why should software only be downloaded from official sources?