Ministry of Education — Approved Curriculum

Programming and Artificial Intelligence

Grade 2 Secondary — Egyptian Baccalaureate

Full Explanation + Question Bank + Model Answers

Chapters 1, 2 & 3 — full notes, questions and answers

Simplified notes with tables and key-point boxes

Over 50 questions per lesson

Chapter test with full model answers

Prepared by **Eng. Mostafa Mohamed**

Contact: **01153464345**

How to Use This Book

This book does not replace the ministry textbook — it **summarises and reorganises** it for revision and exam preparation. Every lesson follows the same four-part structure:

What each lesson contains

- **Learning objectives:** exactly what you must be able to do after studying.
- **Explanation:** the lesson content organised into points and tables, with *Key point* and *Careful — common mistake* boxes.
- **Key terms:** a table of each term with its short definition — the most frequently examined part.
- **Question bank:** fill in the blanks — multiple choice — true/false — matching — classification — explain why — exam-style questions.

Advice before you start

Study the explanation first, then cover the page and answer the question bank **without looking back**. Only then check your answers in the model answers section. The questions you get wrong are exactly what you need to reread.

The four things this chapter examines most

1. The chronological order of the IT development stages, and Moore's Law.
2. The hierarchical relationship between AI, machine learning, deep learning and generative AI.
3. What AI is good at versus what requires caution.
4. The four AI ethics principles, and the difference between accountability, transparency and XAI.

Contents

Chapter 2 — Cyber Security

Lesson 2-1 ..... Cryptographic Technologies and Authentication

Lesson 2-2 ..... Network Security Design

Lesson 2-3 ..... Incident Response and Risk Management

Chapter 3 — Web Applications

Lesson 3-1 ..... The Overall Structure of Web Applications

Lesson 3-2 ..... Web Application Communication Methods

Lesson 3-3 ..... Fundamentals of Frontend Technology

Full course map — all 7 chapters are available in the companion website

Ch. 4 — Web Design and Media: Types of Media · Information Design & UX · Evaluating Websites · Iterative Improvement

Ch. 5 — Data Collection and Cleaning: Collection Methods · Cleaning & Transformation · Open Data and APIs

Ch. 6 — Analysis and Communication: Statistical Inference · Regression Analysis · Visualization & Storytelling

Ch. 7 — Machine Learning and AI: ML Basics · Neural Networks & Deep Learning · LLMs and Generative AI

Chapter 1

Information Technology and Society

This chapter contains four connected lessons: how information technology developed and changed society, what AI is and how it works, where AI is actually used in daily life and industry, and finally what ethical issues arise from its spread. The four lessons build on each other, so do not move on before you have mastered the one before.

1-1 Development of Information Technology and Social Transformation

Learning objectives

- Explain the major stages in the development of information technology and their impact on society.
- Give examples of social changes and emerging technologies, and explain their characteristics.
- Analyse the impact of one information technology on different groups in society, and justify your decision with evidence.

Key fact

At each stage, information technology introduced a **new technology or service** and also changed **how society communicates, works, and does business**.

1. The History of Information Technology (IT)

IT advanced in stages, and devices became **smaller and more connected**. The major stages are summarised below.

Time period	Major technologies and events	Impact on society
1940s–60s	Birth of the computer (ENIAC, vacuum tubes)	Mainly used for military and scientific computation
1970s–80s	Spread of personal computers (PCs)	Beginning of personal computer use
1990s	Commercialization of the Internet; the Web	Globalization of information; spread of email

2000s	Rise of smartphones (iPhone, etc.)	Explosive spread of mobile Internet
2010s onward	Spread of cloud computing	Large-scale data analysis and AI; "IT as a service" becomes widespread

Moore's Law

The **empirical observation** that the number of transistors on an integrated circuit doubles approximately **every two years**. This remained largely accurate for many years, and computing power increased dramatically.

Careful — common mistake

Moore's Law is **not a fixed physical law**; it is an observation about a trend. Miniaturization is now approaching a physical limit, and two problems arise: the **quantum tunneling effect** (electrons slip through barriers) and **leakage current** (current escapes unintentionally), making it difficult to achieve higher performance and lower power consumption at the same time.

In response, new directions for performance improvement are pursued: **parallel processing** using multiple processor cores, and **quantum computers** based on the principles of quantum mechanics.

2. Social Changes Resulting from Information Technology

Change	Definition
SNS (Social Networking Service)	Services that allow users to connect and post and share information. Highly effective at spreading information rapidly.
E-commerce (EC)	Buying and selling goods and services through the Internet. e.g. Amazon, eBay.
Remote work	A working style in which work is performed from home or other remote locations using the Internet.
Online learning	A learning style in which classes and study materials are delivered using the Internet.
Cashless payment	Making payments using electronic money, QR codes, etc., without using cash. e.g. credit cards, debit cards, mobile payment apps.

3. Notable Emerging Technologies

(1) Autonomous driving

A technology that uses AI to drive a vehicle without human operation. It uses **cameras and sensors** to recognize the surroundings, makes driving decisions, and controls the vehicle.

Why edge computing here?

Because a delay of even 0.1 seconds can lead to an accident, **edge computing** is used: processing is performed **instantly on the vehicle itself** rather than sending data to the cloud for judgment and waiting for a reply.

(2) AR / VR

- **AR (Augmented Reality):** overlays digital information **on real-world images**.
- **VR (Virtual Reality):** allows users to **immerse themselves in a virtual space** generated by a computer.

(3) Quantum computing

A technology expected to dramatically speed up computations that are difficult or impossible for traditional computers, by using the principles of quantum mechanics. A classical **bit** holds one state; a **qubit** uses superposition.

Key Terms

Term	Short definition
Moore's Law	The observation that the number of transistors on a chip roughly doubles about every two years.
Edge computing	Processing data on the device itself, instantly, instead of sending it to the cloud.
Cloud computing	IT resources delivered as a service over the Internet.
E-commerce (EC)	Buying and selling goods and services through the Internet.
Remote work	Working from home or another remote location using the Internet.
Online learning	Classes and study materials delivered over the Internet.
SNS	Services connecting users to post and share information rapidly.
Cashless payment	Paying without cash, using electronic money or QR codes.
Quantum tunneling	Effect in which electrons slip through barriers as circuits get very small.
Leakage current	Current that escapes unintentionally in miniaturized circuits.

Lesson summary in 4 lines

1. IT developed in stages: computers → Internet → smartphones → cloud computing.
2. Moore's Law is an observation about transistor doubling every ~2 years, slowed by physical limits.
3. Five social changes: SNS — e-commerce — remote work — online learning — cashless payment.
4. Emerging technologies: autonomous driving — AR/VR — quantum computing.

Question Bank — Lesson 1-1

Part 1: Fill in the blanks

1. The empirical observation that the number of transistors on an integrated circuit doubles approximately every two years is called .....
2. Buying and selling goods and services through the Internet is called .....
3. Performing work from home or another remote location using the Internet is called .....
4. A system for making payments using electronic money and QR codes without cash is called .....
5. The technology that uses AI to drive a vehicle without human operation is .....
6. Processing data on the device itself instantly instead of sending it to the cloud is called .....
7. Computers were born in the ....., and were mainly used for ..... and ..... computation.
8. ..... spread in the 1970s–80s; in the 1990s the ..... was commercialized; and in the 2000s ..... appeared.
9. The technology that spread from the 2010s onward and supports large-scale data analysis is .....
10. The technology that immerses the user in a computer-generated virtual space is ....., while the one that overlays digital information on the real world is .....
11. Two physical problems that appear as transistors get smaller are ..... and .....
12. A classical bit holds one state, while a ..... uses .....

Part 2: Choose the correct answer

1. The correct chronological order of the IT development stages is:

   (a) computer → smartphones → commercial Internet → cloud (b) computer → commercial Internet → smartphones → cloud

   (c) commercial Internet → computer → cloud → smartphones (d) smartphones → commercial Internet → computer → cloud

2. Which of the following is **not** an appropriate description of an emerging technology?
   (a) Autonomous driving uses AI to drive a vehicle (b) AR overlays digital information on real-world images (c) VR is a technology that greatly improves computer processing speed (d) Quantum computing is expected to speed up difficult computations
3. The most appropriate description of the characteristics of SNS:
   (a) A service allowing users to connect, post and share information, highly effective at rapid spreading (b) A service for buying and selling goods online (c) A style in which a person works from home (d) A system for electronic payments without cash
4. The device that filled a whole room in the 1940s was:
   (a) the personal computer (b) the first electronic computer such as ENIAC (c) the smartphone (d) a cloud server
5. The reason autonomous-driving data is processed on the vehicle is:
   (a) to save Internet cost (b) to reduce response time for safety (c) to increase storage (d) to encrypt the data
6. "IT resources delivered as a service over the Internet" describes:
   (a) edge computing (b) quantum computing (c) cloud computing (d) augmented reality
7. The unit that uses the principle of superposition is:
   (a) the bit (b) the byte (c) the qubit (d) the transistor
8. A physical challenge that slows the trend described by Moore's Law is:
   (a) slow Internet (b) leakage current and quantum tunneling (c) high device prices (d) few users
9. Choose **all** that count as emerging technologies:
   (a) email (b) autonomous driving (c) personal computers (d) augmented reality (e) virtual reality (f) quantum computing
10. The stage in which global access to information and email spread is:
    (a) 1940s–60s (b) 1970s–80s (c) 1990s (d) 2010s onward
11. Which is a new direction for performance improvement instead of further miniaturization?
    (a) larger screens (b) parallel processing with multiple cores (c) longer cables (d) more storage
12. "Paying for breakfast with a mobile app" is an example of:
    (a) online learning (b) cashless payment (c) remote work (d) edge computing

Part 3: True (✓) or False (✗) — correct the false statements

1. Moore's Law is the empirical observation that the number of transistors on an integrated circuit doubles approximately every two years. ( )
2. Continued miniaturization faces engineering and physical challenges that slow the trend described by Moore's Law. ( )
3. SNS services are highly effective at spreading information rapidly. ( )
4. E-commerce means buying goods from physical shops using cash. ( )

5. Quantum computing is a general replacement for all classical computers and speeds up every computation. ( )
6. AR places the user completely inside a computer-generated digital environment. ( )
7. The first computers were mainly used for military purposes and scientific computation. ( )
8. Edge computing means sending all data to the cloud to be processed there. ( )
9. Cloud computing made large-scale data analysis and AI more widely available. ( )
10. A qubit and a classical bit work in exactly the same way. ( )

Part 4: Match each description with the correct technology

Description	Options
1) A technology that overlays digital information on real-world images	(a) autonomous driving (b) augmented reality (c) virtual reality
2) A technology that uses AI to drive a vehicle without human operation	
3) A technology allowing users to immerse themselves in a computer-generated space	

Part 5: Classify the following examples

Classify each example under the most suitable category: **(a)** changes in daily life **(b)** changes in industry and the economy **(c)** changes in healthcare and education.

1. Buying products through an online shop.
2. Paying for purchases with a mobile payment app.
3. Sharing photos with friends on a social networking service.
4. A company adopting a work-from-home system.

Part 6: Extended-response questions

1. **Explain why** autonomous-driving data must be processed instantly on the vehicle using edge computing rather than sent to the cloud.
2. **Explain why** Moore's Law is not considered a fixed physical law.
3. **Compare** augmented reality (AR) and virtual reality (VR) in terms of the user's relationship with the real world.
4. **Exam-style question [6 marks]:** Analyse how the spread of cloud computing (2010s onward) changed the way information technology is used. Refer in your answer to large-scale data analysis, AI, and "IT as a service".

5. **In a new context:** A village that had no Internet connection is now connected to high-speed Internet and cashless payment services are available. Predict two changes to daily life, identify one possible new challenge, and explain your answer.

1-2 How AI Works

Learning objectives

- Define AI and distinguish between machine learning, deep learning and generative AI.
- Explain the relationship between these concepts using suitable examples.
- Evaluate the risk of **hallucination** and identify an appropriate way to verify generative AI output.

Key fact

AI is a **broad field**. Machine learning, deep learning and generative AI are **related concepts inside it**, not completely separate technologies.

1. What is Artificial Intelligence (AI)?

AI is a field covering computer systems that can perform tasks such as **learning from data**, **prediction**, **recognition**, **content generation**, and **making or supporting decisions**. Everyday examples: speech recognition, image recognition, and translation.

Good to know

Most current AI systems are **narrow AI**: designed for a specific task or a limited set of tasks, not a general intelligence that can do everything.

2. The Relationship Between the Four Concepts

The essential difference: a traditional system relies on **explicitly programmed rules**, while machine learning relies on **patterns the model learns from data**.

The hierarchy examiners ask about

AI > Machine Learning > Deep Learning > Generative AI

Machine learning is **a branch of** AI, deep learning is **a method within** machine learning, and **most** modern generative AI applications are built on deep learning models.

Careful

This is a **simplified teaching relationship** and should not be read as a **strict containment hierarchy in every case**. Also: AI and machine learning do **not** mean the same thing, and deep learning is **not a completely different technology** from machine learning — it is a type of it.

Term	Definition	Examples
Artificial Intelligence (AI)	A field of computer systems performing tasks such as learning, prediction, recognition, content generation and decision support.	Speech and image recognition, translation
Machine Learning (ML)	A branch of AI in which models learn patterns from data to make predictions or classifications, instead of every rule being programmed explicitly.	Spam filtering, product recommendation
Deep Learning (DL)	A machine-learning method based on **multi-layer neural networks**, able to learn complex representations and patterns.	Image analysis, speech recognition
Artificial Neural Network (ANN)	A computational model loosely inspired by connected neurons, made of connected units whose **weights change during training**.	The basis of deep learning models
Generative AI (GenAI)	Systems that create **new content** (text, images, audio, software) based on patterns learned from training data.	ChatGPT, image generators

3. Hallucination

A concept that appears often in exams

Generative AI can produce text that **looks plausible but is factually wrong** — this is called hallucination. It is therefore risky to use its output directly as an answer for a school report; the learner must **verify the output and its sources** before using it.

Why does AI struggle with rare things?

Deep learning needs **relatively large amounts of data** to learn reliable patterns. If something is rare in the training data, the model finds it hard to recognise accurately.

Key Terms

Term	Short definition
AI	The general field of systems performing tasks such as learning, prediction and generation.
Machine learning	Learns patterns from data instead of following explicitly programmed rules.
Deep learning	Uses multi-layer neural networks; often needs relatively large data.
Neural network (ANN)	A computational model inspired by connected neurons, used to learn from data.
Generative AI	Uses deep learning to generate new data such as text, images and audio.
Hallucination	Producing information that sounds convincing but is incorrect or unsupported.
Narrow AI	AI designed for a specific task or limited set of tasks.

Lesson summary in 4 lines

1. AI is the broad field; machine learning sits inside it; deep learning sits inside machine learning.
2. Current generative AI is built on deep learning — broadest idea to most specialised.
3. The essential difference: explicitly programmed rules ← versus → patterns learned from data.
4. Hallucination is the main risk of generative AI; the remedy is verifying output and sources.

Question Bank — Lesson 1-2

Part 1: Fill in the blanks

1. The general term for computer systems able to perform tasks such as learning, recognition, prediction and content generation is .....
2. The branch of AI in which models learn patterns from data is .....
3. The machine-learning method based on multi-layer neural networks is called .....
4. AI systems that create new content are called .....
5. The computational model loosely inspired by connected neurons is called .....
6. When generative AI produces information that looks plausible but is factually wrong, this is called .....
7. Most current AI systems are ..... AI, meaning they are designed for a specific task.

8. The ..... of the connected units in a neural network change during ..... so it can learn patterns from data.
9. Three tasks AI can perform according to the lesson definition are ....., ... and .....
10. Deep learning needs ..... data in order to learn reliable patterns.

Part 2: Choose the correct answer

1. Which option correctly describes the relationship between the four concepts?
   (a) AI > deep learning > machine learning > generative (b) machine learning > AI > generative > deep learning
   (c) AI > machine learning > deep learning > generative (d) generative > deep learning > machine learning > AI
2. Which of the following is **not** an appropriate example of generative AI?
   (a) ChatGPT (b) an image-generating AI (c) a spam filter (d) an audio-generating AI
3. The most appropriate description of the relationship between the concepts:
   (a) Machine learning is a type of AI, and deep learning is a type of machine learning (b) AI is a type of machine learning
   (c) Deep learning and machine learning are completely different technologies (d) Generative AI generates data without using machine learning
4. "Spam filtering" and "product recommendation" are examples of:
   (a) machine learning (b) generative AI (c) quantum computing (d) augmented reality
5. What distinguishes deep learning from other machine-learning methods?
   (a) it needs no data (b) it uses multi-layer neural networks (c) it relies on explicitly programmed rules (d) it is always faster
6. The most appropriate action when using generative AI output in a school report:
   (a) copy it as it is (b) verify its accuracy and its sources (c) regenerate it many times (d) translate it into another language
7. A farmer wants a system that distinguishes healthy crops from diseased ones in photographs. The most suitable training data is:
   (a) texts about agriculture (b) labelled images of healthy and diseased crops (c) market prices (d) weather data only
8. "Overlapping categories" describes:
   (a) the four concepts being completely independent (b) each concept sitting inside the broader one (c) the concepts meaning the same thing (d) their chronological order
9. The essential difference between a rule-based system and machine learning is:
   (a) speed of the processor (b) explicit rules versus patterns learned from data (c) screen size (d) programming language used
10. "Recognising pedestrians on the road in autonomous driving" is best classified as:
    (a) deep learning (b) generative AI (c) quantum computing (d) cashless payment

Part 3: True (✓) or False (✗) — correct the false statements

1. Machine learning is one of the technologies that make AI work. ( )
2. Deep learning is a completely different technology from machine learning. ( )
3. Generative AI uses deep learning to generate new data. ( )
4. AI and machine learning have the same meaning. ( )
5. Most current AI systems are general-purpose and can perform any task. ( )
6. Generative AI output is always correct as long as it is written in fluent language. ( )
7. The weights in a neural network change during training. ( )
8. The four concepts should be understood as a strict containment hierarchy in every case. ( )

Part 4: Match each description with the correct term

Description	Options
1) A technology that learns patterns from data to make predictions and judgments	(a) machine learning (b) deep learning (c) generative AI
2) A technology that uses neural networks to learn complex patterns	
3) An AI technology that generates new data such as text and images	

Part 5: Classify each example

Classify each example under the most suitable category: **(a)** machine learning **(b)** deep learning **(c)** generative AI.

1. Automatically classifying spam email.
2. Recognising pedestrians on the road in autonomous driving.
3. Automatically generating new images from a text prompt.
4. Recommending products based on a user's purchase history.

Part 6: Extended-response questions

1. **Explain why** AI may struggle with something it has rarely seen in its training data.
2. **Explain why** it is risky to use generative AI output directly as the answer for a school report.
3. **What do** a spam filter and a product recommendation system have in common, despite doing different tasks?

4. **Exam-style question [6 marks]:** Analyse the relationship between AI, machine learning, deep learning and generative AI. Use the idea of **overlapping categories**, and give one example of each.
5. **In a new context:** A farmer wants to use an AI system to distinguish healthy crops from diseased ones in photographs. Explain what kind of data the system needs for training, and identify one factor that could make its prediction wrong.

1-3 AI in Daily Life and Industry

Learning objectives

- Give examples of how AI is used in daily life and in different industries.
- Explain what AI is good at and what requires caution when using it.
- Evaluate a use in a specific context, and justify the need for human oversight when the impact of an error is high.

Key fact

AI is **good at finding patterns in data**, but **human judgment is still necessary** where ethics, privacy and responsibility are involved.

1. AI in Daily Life

Service	What the AI does	Examples
Recommendation systems	Predict preferences from past behaviour data and display recommendations.	YouTube, Amazon, Spotify
Voice assistants	Recognise speech, understand commands, and carry them out.	Siri, Google Assistant
Machine translation	Automatically translate text into different languages.	Google Translate, DeepL
Face recognition	Automatically detect and recognise people's faces in images.	Unlocking a smartphone

2. Use of AI in Industry

Industry	Examples of use

Healthcare	AI image diagnosis (detecting disease from X-ray and CT images), and supporting drug discovery.
Agriculture	Predicting the harvest time, and detecting pests and diseases.
Manufacturing	Automating product quality inspection, and **predictive maintenance** (predicting machine failures before they occur).
Logistics	Optimising delivery routes.

3. Characteristics of AI and Precautions for Use

This is the most important part of the lesson; it appears in exams as "choose what AI is good at" or "choose the one that does not belong".

What AI is good at

- Finding and classifying **patterns** in complex data such as images and text.
- Recognising images, sounds and text, and generating some kinds of content.
- **Probabilistic inference and prediction** based on data.

What requires caution when using AI

- **Ethical** decisions that may lead to discrimination or bias.
- Handling **personal information** and sensitive data.
- **High-impact** decisions and determining **responsibility** for their outcomes.
- Accuracy when training data is **insufficient, unrepresentative or biased**.
- Generating incorrect or unsupported information that sounds convincing (**hallucination**).
- Rights issues when **copyrighted** works are used as training data.
- Loss of clarity about how a judgment was reached (**the black box problem**).

A golden rule for answering

The higher the **impact of an error** or the **seriousness of the decision**, the greater the need for **human review**. That is why a final diagnosis must be confirmed by a **human doctor** and not left to AI alone.

Key Terms

Term	Short definition

Recommendation system	Predicts preferences from past behaviour data and shows recommendations.
Voice assistant	Recognises speech, understands commands and executes them.
Machine translation	Automatically translates text into different languages.
Face recognition	Automatically detects and recognises faces in images.
Predictive maintenance	Using data to predict machine or equipment failures before they occur.
Black box problem	When it is unclear how the AI reached its judgment.

Lesson summary in 4 lines

1. Daily life: recommendations — voice assistants — machine translation — face recognition.
2. Industry: healthcare — agriculture — manufacturing — logistics.
3. Good at: patterns, recognition, probabilistic prediction.
4. Requires caution: ethics, privacy, the final decision and responsibility.

Question Bank — Lesson 1-3

Part 1: Fill in the blanks

1. The system that predicts preferences from past behaviour data and displays recommendations is called a .....
2. The AI technology that recognises speech, understands commands and executes them is a .....
3. AI image-diagnosis systems are used in the ..... industry.
4. In manufacturing, using data to predict machine failures before they occur is called .....
5. When it is unclear how the AI reached its judgment, this is called the .....
6. The technology that converts text in a foreign language into your own language is .....
7. In logistics, AI is used for .....
8. In agriculture, AI is used for ..... and .....
9. AI judgments can become inaccurate when training data is ..... or .....
10. Producing convincing but incorrect information is called .....

Part 2: Choose the correct answer

1. Which of the following does **not** belong to "what requires caution when using AI"?
   (a) ethical judgments (b) finding and classifying patterns (c) judgments involving personal information (d) making the final decision
2. Choose **all** the things AI is good at:
   (a) ethical judgments (b) finding and classifying features in images and text (c) judgments involving personal information
   (d) probabilistic inference and prediction (e) making decisions and bearing responsibility for outcomes (f) recognising and generating images, sound and text
3. Which of the following is **not** an appropriate description of an AI service?
   (a) A recommendation system predicts preferences from past behaviour (b) A voice assistant recognises speech and executes commands
   (c) Machine translation is a system in which humans translate foreign languages manually (d) Face recognition automatically detects people's faces
4. "Detecting disease from X-ray images" belongs to:
   (a) healthcare (b) agriculture (c) manufacturing (d) logistics
5. "Automating product quality inspection" belongs to:
   (a) healthcare (b) agriculture (c) manufacturing (d) logistics
6. Choose **all** that require caution when using AI:
   (1) high-speed processing of large amounts of data (2) ethical judgments (3) judgments involving personal information (4) recognising images and sound
7. A school library wants to recommend books based on what a student borrowed before. The system used is:
   (a) machine translation (b) a recommendation system (c) face recognition (d) predictive maintenance
8. The main reason a human doctor must review an AI diagnosis is:
   (a) the system is slow (b) the impact of an error on the patient is high (c) the system is expensive (d) the device is hard to operate
9. A rights issue connected to AI training data is:
   (a) electricity cost (b) use of copyrighted works as training data (c) screen resolution (d) network speed
10. "Optimising delivery routes" belongs to:
    (a) healthcare (b) agriculture (c) manufacturing (d) logistics

Part 3: True (✓) or False (✗) — correct the false statements

1. AI is good at probabilistic inference and prediction based on data. ( )
2. AI is good at recognising images and sound. ( )
3. It is fine to leave ethical judgments entirely to AI. ( )
4. AI judgments can become inaccurate when the training data is biased. ( )

5. Machine translation means humans translating foreign texts manually. ( )
6. Predictive maintenance is used in manufacturing to predict equipment failures before they occur. ( )
7. The black box problem means the AI processes data too slowly. ( )
8. The higher the impact of an error, the greater the need for human review. ( )

Part 4: Match each service with the technology used

Service	Options
1) YouTube suggests videos that match the user's preferences	(a) recommendation system (b) voice assistant (c) machine translation (d) face recognition
2) Speaking to a smartphone to check the weather	
3) Translating a foreign-language website into your own language	
4) A smartphone camera automatically detecting a person's face	

Part 5: Identify the most closely related industry

Options: **(a)** healthcare **(b)** agriculture **(c)** manufacturing **(d)** logistics.

1. Optimising delivery routes.
2. Detecting disease from X-ray images.
3. Detecting pests and diseases.
4. Automating product quality inspection.

Part 6: Extended-response questions

1. **Explain why** a final diagnosis should be confirmed by a human doctor rather than left to AI alone.
2. **Explain why** AI services raise privacy concerns.
3. **Exam-style question [6 marks]:** Analyse why AI suits some tasks while requiring caution in others. Refer to what it is good at (finding patterns, recognition, prediction) and to what requires caution (ethical judgments, privacy, making the final decision).
4. **In a new context:** A school library wants to use AI to recommend books to students based on what they borrowed before. Explain how the system would work, and identify one precaution the school should take.

1-4 Ethical Issues with AI

Learning objectives

- Explain what algorithmic bias is and describe its main causes.
- Link the core AI ethics principles (fairness, transparency, privacy protection, accountability) to specific situations.
- Evaluate an ethical situation, justify a rule for responsible use, and identify the parties who bear responsibility.

Key fact

If **training data is biased**, AI can **reproduce that bias** in its judgments. Responsible use means: **checking for bias**, **being able to explain decisions**, and **knowing who is responsible**.

1. Algorithmic Bias

Definition: a deviation or pattern in AI output that may lead to **unfair or harmful outcomes**. It can arise from the **data**, the **system design**, the **way it is used**, or the **human and social context**.

Examples: a hiring system that unfairly favours one group, or a face-recognition system that is less accurate for certain groups.

Main causes of bias

- **Biased training data:** insufficient data about certain attributes, or past discriminatory tendencies reflected in the data.
- **How the system is built:** unsuitable choice of variables, a **proxy variable** that indirectly represents a protected attribute, or the model design itself.

Careful

Algorithmic bias is **not caused by computer processing speed** or weak hardware. Its causes are the data, the design, or the use.

2. Privacy Issues

1. **Surveillance through face-recognition technology:** cameras in public places can identify and track individuals.
2. **Mass collection of personal data:** large amounts of online behaviour data are collected and analysed.

Privacy here means: control over which personal data is shared.

3. Explainable AI (XAI) and Responsibility

Term	Explanation
Explainable AI (XAI)	Methods that help people understand the **factors** that contributed to a system reaching a particular output or decision. When the route to a result is unclear, it is hard to evaluate it or to detect errors or bias.
Responsibility	Defining the roles and duties of the parties involved in developing, operating and using the system (developer, operator, user). No single allocation fits every context.
Accountability	Identifying the parties responsible for the system, its decisions and its effects, so that they **can be held to account** according to their roles.
Transparency	Providing clear and appropriate information about the system, its use, the decision process and its limitations.

A fine distinction that is examined often

Accountability is not the ability to explain a decision — that is the job of **XAI**. Accountability identifies **who is answerable** for the outcome.

4. The Four AI Ethics Principles

Principle	Description
Fairness	Not unjustly discriminating against any person or particular group.
Transparency	Providing clear, appropriate information about the system, its use, the decision process and its limitations.
Privacy protection	Handling personal information appropriately and protecting it.
Accountability	Identifying the parties responsible for the system, its decisions and effects, so they can be held to account.

A quick way to tell them apart in an exam

- Talk of **discrimination or unfair treatment of a group** → fairness.
- Talk of **disclosure, clarity, explaining the decision process** → transparency.
- Talk of **personal data** or using it beyond its original purpose → privacy protection.
- Talk of **who is responsible and who is held to account** → accountability.

Key Terms

Term	Short definition
Algorithmic bias	A pattern in AI output that may lead to unfair or harmful outcomes.
Training data	The examples a system learns its patterns from; the less representative they are, the higher the risk of bias.
Proxy variable	A variable that indirectly represents a protected attribute.
XAI	Technology allowing people to understand why AI made a particular judgment.
Black box problem	Lack of clarity about how the system reached its judgment.
Fairness	Not unjustly discriminating against a person or group.
Transparency	Showing the AI decision process clearly.
Privacy protection	Handling and protecting personal information appropriately.
Accountability	Identifying responsible parties who can be held to account.

Lesson summary in 4 lines

1. Algorithmic bias arises from data, design, use or context — not from computer speed.
2. Privacy issues: surveillance by face recognition + mass data collection.
3. XAI explains "why"; accountability determines "who is answerable".
4. The four principles: fairness — transparency — privacy protection — accountability.

Question Bank — Lesson 1-4

Part 1: Fill in the blanks

1. A pattern in an AI system that may lead to unfair or harmful outcomes is called .....
2. The technology allowing people to understand why AI made a particular judgment is ....., abbreviated .....
3. The principle requiring that no person or group is unjustly discriminated against is .....
4. The principle requiring appropriate handling of personal information is .....
5. The examples a system learns its patterns from are called .....
6. Identifying the parties responsible for a system and its decisions so they can be held to account is .....

7. Lack of clarity about how AI reached its judgment is called the .....
8. Two privacy issues are ..... through face recognition and ..... of personal data.
9. A variable that indirectly represents a protected attribute is called a .....
10. The three parties whose responsibility must be defined are the ....., the ..... and the .....

Part 2: Choose the correct answer

1. Which of the following is **not** an appropriate cause of algorithmic bias?
   (a) biased training data (b) past discriminatory tendencies reflected in the data (c) slow computer processing speed (d) insufficient data about certain attributes
2. Choose **all** that represent AI-related privacy issues:
   (a) identifying and tracking individuals with face recognition (b) collecting and analysing large amounts of online behaviour data
   (c) AI creating artistic works (d) AI computing speed improving
3. The most appropriate description of ethical issues with AI:
   (a) there are no ethical issues (b) bias is caused by processing speed
   (c) bias in training data can cause discriminatory bias in judgments (d) an unclear decision is not a problem for users
4. "Ensuring a hiring AI evaluates fairly regardless of gender" relates to the principle of:
   (a) fairness (b) transparency (c) privacy protection (d) accountability
5. "Not using collected personal data for purposes other than the original one" relates to:
   (a) fairness (b) transparency (c) privacy protection (d) accountability
6. "Being able to explain why a particular diagnostic result was reached" relates mainly to:
   (a) fairness (b) transparency and XAI (c) privacy protection (d) processing speed
7. The difference between accountability and XAI is that accountability:
   (a) explains the decision process (b) identifies who is answerable for the outcome (c) speeds up the system (d) collects the data
8. A face-recognition system that is less accurate for certain groups is an example of:
   (a) hallucination (b) algorithmic bias (c) edge computing (d) predictive maintenance
9. A single fixed allocation of responsibility that fits every context:
   (a) exists and is defined by law everywhere (b) does not exist; it varies by system and context (c) always falls on the user (d) always falls on the developer
10. The problem that transparency and XAI are meant to address is:
    (a) high cost (b) the black box problem (c) slow networks (d) small datasets

Part 3: True (✓) or False (✗) — correct the false statements

1. Algorithmic bias is a pattern in AI output that may arise from the data, the system design or the way it is used. ( )

2. Even if the AI decision process is unclear, there is no problem as long as the result is correct. ( )
3. XAI is a technology that allows people to understand the AI's reasoning. ( )
4. When AI makes a wrong judgment, the responsible party has already been clearly defined in every case. ( )
5. Transparency means providing clear information about the system, the decision process and its limitations. ( )
6. Training data that does not represent reality increases the chance of biased output. ( )
7. Algorithmic bias is caused by weak hardware. ( )
8. Privacy means control over which personal data is shared. ( )

Part 4: Match each description with the correct principle

Description	Options
1) Not unjustly discriminating against any person or particular group	(a) fairness (b) transparency (c) privacy protection (d) accountability
2) Providing clear information about the system, its use, the decision process and its limits	
3) Handling personal information appropriately and protecting it	
4) Identifying the parties responsible for AI outcomes so they can be held to account	

Part 5: Extended-response questions

1. **Explain why** an AI system may reproduce discrimination that exists in society.
2. **Explain why** it is difficult to evaluate an AI result when the route to it is unclear.
3. **What is the difference** between transparency and accountability?
4. **Exam-style question [6 marks]:** Analyse how algorithmic bias can arise in an AI system and how it can be reduced. Refer to the cause of bias (biased or insufficient training data) and to how the principles of fairness and transparency help address it.
5. **In a new context:** A school wants to use face-recognition cameras at its gate to record attendance automatically. Identify one practical benefit and one privacy concern. Then, if the camera misidentifies a student, who should be responsible — the school or the manufacturer? Give a reason.

Chapter Test

Chapter 1 — Information Technology and Society

Instructions

Time: 1 hour · Total marks: 40 · Answer all questions · Write your answers on a separate sheet, then mark yourself using the model answers.

Question 1: Choose the correct answer [10 marks]

1. The stage in which electronic computers appeared and were used for military purposes is:
   (a) 1940s–60s (b) 1970s–80s (c) 1990s (d) 2000s
2. Processing data on the device itself instead of sending it to the cloud is called:
   (a) cloud computing (b) edge computing (c) quantum computing (d) deep learning
3. The correct relationship between the concepts is:
   (a) AI > ML > DL > generative (b) ML > AI > DL > generative (c) DL > AI > ML > generative (d) generative > AI > DL > ML
4. Which of the following is AI good at?
   (a) ethical judgments (b) bearing responsibility for outcomes (c) probabilistic inference and prediction (d) deciding who is answerable
5. A main cause of algorithmic bias is:
   (a) a slow processor (b) insufficient training data about certain attributes (c) a small screen (d) weak Internet
6. "Providing clear information about the system, the decision process and its limits" defines:
   (a) fairness (b) transparency (c) privacy protection (d) accountability
7. The technology that overlays digital elements on a real-world scene is:
   (a) VR (b) AR (c) XAI (d) SNS
8. "Predictive maintenance" belongs to:
   (a) healthcare (b) agriculture (c) manufacturing (d) logistics
9. Generative AI producing plausible but incorrect text is called:
   (a) bias (b) hallucination (c) transparency (d) accountability
10. Moore's Law describes transistor count doubling roughly every:
    (a) six months (b) one year (c) two years (d) ten years

Question 2: Fill in the blanks [8 marks]

1. Buying and selling goods and services over the Internet is called .....
2. The computational model inspired by connected neurons is the .....
3. The system that predicts preferences from past behaviour data is a .....
4. Lack of clarity about how a system reached its judgment is the .....
5. The unit that uses the principle of superposition is the .....
6. The examples a system learns its patterns from are called .....
7. The AI technology that converts foreign-language text into your own language is .....
8. The principle requiring that no group is unjustly discriminated against is .....

Question 3: True (✓) or False (✗) — correct the false statements [6 marks]

1. Quantum computing speeds up all types of computation and replaces classical computers. ( )
2. Deep learning is a method within machine learning. ( )
3. Ethical judgments can be left entirely to AI. ( )
4. Edge computing reduces response time in autonomous driving. ( )
5. Accountability is the ability to explain how the system reached its decision. ( )
6. SNS services are effective at spreading information rapidly. ( )

Question 4: Match the two columns [4 marks]

(A)	(B)
1) Predicting harvest time and detecting pests	(a) manufacturing (b) agriculture (c) logistics (d) healthcare
2) Optimising delivery routes	
3) Image diagnosis and drug discovery	
4) Automating product quality inspection	

Question 5: Extended response [12 marks]

1. **[4 marks]** Explain why human oversight is necessary when AI is used to diagnose disease from X-ray images.
2. **[4 marks]** Compare **augmented reality** and **virtual reality**, and give one example of a use of either.
3. **[4 marks]** Analyse how algorithmic bias can arise in a hiring system, and how the principle of transparency helps detect it.

Model Answers

Chapter 1 question banks and chapter test

Lesson 1-1 — Answers

Part 1: Fill in the blanks

1) Moore's Law. **2)** E-commerce. **3)** Remote work. **4)** Cashless payment. **5)** Autonomous driving. **6)** Edge computing. **7)** 1940s — military — scientific. **8)** Personal computers — Internet — smartphones. **9)** Cloud computing. **10)** Virtual reality — augmented reality. **11)** Quantum tunneling — leakage current. **12)** Qubit — superposition.

Part 2: Multiple choice

1) b **2)** c **3)** a **4)** b **5)** b **6)** c **7)** c **8)** b **9)** b, d, e, f **10)** c **11)** b **12)** b

Note on (2): VR immerses the user in a digital environment; it has nothing to do with improving processing speed.

Part 3: True / False

1) ✓ **2)** ✓ **3)** ✓ **4)** ✗ — e-commerce is buying and selling **over the Internet**, not in physical shops with cash. **5)** ✗ — quantum computing is **not a general replacement**; it may help with specific classes of problems.

6) ✗ — that describes **VR**; AR adds digital elements to the real world. **7)** ✓ **8)** ✗ — edge computing means processing **on the device itself**, not in the cloud. **9)** ✓ **10)** ✗ — a bit holds one state while a qubit uses **superposition**.

Parts 4 and 5

Part 4: **1)** b **2)** a **3)** c

Part 5: **1)** b (industry and the economy) **2)** a **3)** a **4)** b. Sample reasoning: paying by mobile app changes an individual's everyday buying behaviour, so it is a change in daily life.

Part 6: Extended response

1) Because a delay of even a fraction of a second can affect **safety**. Sending data to the cloud and waiting for a reply increases response time, whereas edge computing processes the data locally and reduces that delay.

2) Because it is an **empirical observation** about a historical trend, not a fixed physical rule, and it faces engineering and physical limits (leakage current, quantum tunneling) that slow it down.

3) AR adds digital elements **on top of** a real scene, so the user stays in the real world; VR places the user **inside** a fully computer-generated environment.

4) Answer points: the cloud made IT resources available **as a service over the Internet** instead of owning hardware; it provided storage and processing capacity that enabled **large-scale data analysis**; it allowed AI models to be trained and run at scale; so access to digital services became faster and cheaper.

5) Sample: two changes — online shopping and payment become common, and remote learning or work becomes possible. Possible challenge — excluding people without a bank card or smartphone, or new security and fraud risks.

Lesson 1-2 — Answers

Part 1: Fill in the blanks

1) Artificial intelligence. **2)** Machine learning. **3)** Deep learning. **4)** Generative AI. **5)** Artificial neural network. **6)** Hallucination. **7)** Narrow. **8)** Weights — training. **9)** Learning from data — prediction — recognition (also generation and decision support). **10)** Relatively large.

Part 2: Multiple choice

1) c **2)** c **3)** a **4)** a **5)** b **6)** b **7)** b **8)** b **9)** b **10)** a

Part 3: True / False

1) ✓ **2)** ✗ — deep learning is **a type of** machine learning, not different from it. **3)** ✓ **4)** ✗ — AI is the **broader** concept; machine learning is one technology within it. **5)** ✗ — most are **narrow** AI. **6)** ✗ — it may be a **hallucination**: plausible but incorrect. **7)** ✓ **8)** ✗ — it is a **simplified teaching relationship**, not a strict hierarchy in every case.

Parts 4 and 5

Part 4: **1)** a **2)** b **3)** c

Part 5: **1)** a **2)** b **3)** c **4)** a. Reasoning: recognising pedestrians relies on analysing complex images, a deep-learning task.

Part 6: Extended response

1) Because models learn from **many examples**; if something is rare in the training data the model does not find enough patterns to recognise it accurately.

2) Because it may produce information that sounds convincing but is **incorrect or unsupported** (hallucination), so the student would pass on a false fact. The correct approach is to verify the output and its sources.

3) Neither works from explicitly programmed rules; both **learn patterns from data** in order to predict or classify — so both are machine-learning applications despite the different tasks.

4) Answer points: AI is the broad category (example: translation) → machine learning sits inside it and learns patterns from data (example: spam filtering) → deep learning sits inside machine learning and uses multi-layer neural networks (example: speech recognition) → most generative systems are built on deep learning (example: image generation). Note that this is a simplified relationship, not a strict hierarchy.

5) It needs **labelled images** of healthy and diseased crops, in sufficient numbers and under varied photographic conditions. A factor that could make the prediction wrong: too few examples of a particular disease, or lighting/crop types different from the training data.

Lesson 1-3 — Answers

Part 1: Fill in the blanks

1) Recommendation system. **2)** Voice assistant. **3)** Healthcare. **4)** Predictive maintenance. **5)** Black box problem. **6)** Machine translation. **7)** Optimising delivery routes. **8)** Predicting harvest time — detecting pests and diseases. **9)** Insufficient/unrepresentative — biased. **10)** Hallucination.

Part 2: Multiple choice

1) b **2)** b, d, f **3)** c **4)** a **5)** c **6)** 2 and 3 **7)** b **8)** b **9)** b **10)** d

Part 3: True / False

1) ✓ **2)** ✓ **3)** ✗ — its judgments may lead to discrimination or bias, so ethical judgments are not left entirely to AI. **4)** ✓ **5)** ✗ — machine translation is done **automatically** by the system, not manually. **6)** ✓ **7)** ✗ — the black box problem is about **lack of clarity in how a judgment was reached**, not speed. **8)** ✓

Parts 4 and 5

Part 4: **1)** a **2)** b **3)** c **4)** d

Part 5: **1)** d **2)** a **3)** b **4)** c

Part 6: Extended response

1) Because the decision is **high-impact** and affects the patient's life; the system may err if its data is insufficient or biased, and determining responsibility for a mistake requires a final human decision.

2) Because they use **personal data** — what you watch, buy and say — to deliver their services, which raises the question of who controls that data and how it is used.

3) Answer points: AI is good at finding and classifying patterns in complex data, recognising images, sound and text, and probabilistic inference and prediction — because these are tasks that can be learned from many examples. Caution is required for ethical judgments (risk of discrimination), personal data (privacy), and the final decision and responsibility — because these need values and human judgment that

cannot be derived from patterns. The higher the impact of an error, the greater the need for human oversight.

4) It works as a recommendation system: it analyses the student's borrowing history, predicts similar books matching their preferences, and displays them. Precaution: protecting the privacy of borrowing data, avoiding narrowing the student to one type of book, or having the librarian review the recommendations.

Lesson 1-4 — Answers

Part 1: Fill in the blanks

1) Algorithmic bias. **2)** Explainable AI — XAI. **3)** Fairness. **4)** Privacy protection. **5)** Training data. **6)** Accountability. **7)** Black box problem. **8)** Surveillance — mass collection. **9)** Proxy variable. **10)** Developer — operator — user.

Part 2: Multiple choice

1) c **2)** a, b **3)** c **4)** a **5)** c **6)** b **7)** b **8)** b **9)** b **10)** b

Part 3: True / False

1) ✓ **2)** ✗ — when the process is unclear it is **hard to verify** whether the result is correct. **3)** ✓ **4)** ✗ — the allocation of responsibility **varies** depending on whether the party is developer, operator or user, and is not settled in every context. **5)** ✓ **6)** ✓ **7)** ✗ — bias comes from data, design, use or context, **not hardware**. **8)** ✓

Part 4: Matching

1) a **2)** b **3)** c **4)** d

Part 5: Extended response

1) Because it learns from **training data** that may reflect past discriminatory tendencies or under-represent some groups, so it reproduces the same pattern in its output.

2) Because lack of clarity about how the result was reached (the black box problem) prevents errors or bias from being detected, so the correctness or fairness of the result cannot be judged.

3) **Transparency** = providing clear information about the system, the decision process and its limits. **Accountability** = identifying the responsible parties so they can be held to account for the outcome. In short: transparency answers "how and why", accountability answers "who is answerable".

4) Answer points: bias arises from biased or insufficient training data about certain attributes, from the system design (a proxy variable representing a protected attribute), or from how it is used. To reduce it: apply **fairness** by checking how well the data represents different groups and testing outcomes across them, and apply **transparency** by disclosing the decision process and the system's limits so it can be reviewed and bias detected.

5) Sample: benefit — fast, accurate attendance recording without queues. Concern — collecting students' biometric data and the possibility of tracking them. Responsibility — shared: the school is responsible for the decision to use it, for protecting the data and for providing an alternative when errors occur; the manufacturer is responsible for the system's accuracy and for testing it across diverse groups.

Chapter Test — Answers

Question 1

1) a **2)** b **3)** a **4)** c **5)** b **6)** b **7)** b **8)** c **9)** b **10)** c

Question 2

1) E-commerce. **2)** Artificial neural network. **3)** Recommendation system. **4)** Black box problem. **5)** Qubit. **6)** Training data. **7)** Machine translation. **8)** Fairness.

Question 3

1) ✗ — it helps with **specific classes** of problems and is not a general replacement. **2)** ✓ **3)** ✗ — they may lead to discrimination or bias, so human judgment is required. **4)** ✓ **5)** ✗ — that is the role of **XAI**; accountability identifies **who is answerable**. **6)** ✓

Question 4

1) b **2)** c **3)** d **4)** a

Question 5

1) Because the decision is high-impact and affects the patient's health; the system may err if training data is insufficient or unrepresentative, its decision process may be unclear (black box), and responsibility for the final diagnosis must rest clearly with the doctor.

2) AR adds digital elements to a real-world scene, so the user stays in their surroundings; VR places the user inside a fully computer-generated environment. Example: using AR to display information over a museum artefact.

3) Bias arises if the system is trained on past hiring data reflecting an unfair preference for one group, or if a proxy variable indirectly represents a protected attribute. **Transparency** helps detect it because it provides clear information about the decision process and the system's limits, so the criteria used can be reviewed and outcomes tested across different groups.

Chapter 2

Cyber Security

This chapter moves from protecting **the connection and the account** (2-1), to protecting **the network itself** with a layered design (2-2), and finally to what happens **after a breach actually occurs**: incident response and risk management (2-3). The idea running through the whole chapter: **security does not come from one technology, but from layers working together**.

2-1 Cryptographic Technologies and Authentication

Learning objectives

- Explain how HTTPS communication uses different technologies to protect a connection.
- Distinguish the roles of encryption, digital certificates, multi-factor authentication and digital signatures.
- Evaluate an authentication method in a given context and justify your choice against security and accessibility needs.

Key fact

Safe online communication and services are achieved by **combining encryption and authentication**, not by any single technology.

1. How HTTPS Communication Works

HTTPS is HTTP carried over a secured **TLS** connection. TLS provides three things: **confidentiality** of the data, **integrity** while it travels, and **verification** of the server's identity and domain name. The steps that establish the secure connection are called the **TLS handshake**.

Stage	What happens	Main protection mechanism
1) TLS handshake: certificate check	The server sends its digital certificate; the browser checks its validity, its chain of trust and that it matches the site name.	Public-key cryptography
2) TLS handshake: key sharing	The two sides agree on shared secrets from which session keys are derived, without the key itself being sent across the network.	Public-key cryptography

3) Data exchange	Session data is protected using common-key cryptography together with integrity mechanisms.	Common-key cryptography

Why two kinds of cryptography in one connection?

Public-key cryptography is used to **share keys safely** — it solves the problem of "how do we agree on a secret without sending it". **Common-key cryptography** is then used to **exchange large amounts of data quickly**. This division of roles achieves both security and communication speed; exchanging all data with public-key cryptography would be far too slow.

Public-key cryptography uses a **pair of linked keys**: a public key and a private key.

2. Use of Authentication in Real Services

Many services adopt **multi-factor authentication (MFA)**, in which two or more of the **three factors of authentication** are combined:

- **Knowledge** — something you know (a password).
- **Possession** — something you have (a phone, a smart card, a one-time code).
- **Biometric** — something you are (a fingerprint, a face).

When only one factor is used, an unauthorized party can gain access if that factor is broken. By combining multiple factors, even if one is broken, another can still prevent access. For example, if only a password (knowledge) is used, an unauthorized login becomes possible once the password is leaked; but if a notification to a smartphone (possession) is also required, an attacker cannot log in without the device.

Service	Examples of authentication used
Online banking	Password (knowledge) + one-time password (possession)
SNS login	Password (knowledge) + SMS authentication (possession)
Company laptop login	Smart card (possession) + fingerprint authentication (biometric)
Online shopping	Password (knowledge) + one-time code from 3-D Secure (possession)

Careful — a frequently examined mistake

"Password + a second password" or "password + a secret question" is **not** multi-factor authentication, because both factors belong to the same **knowledge** category. Multi-factor authentication requires factors from **different categories**.

3. Combinations of Security Technologies

Technology	Effect
Encryption (common-key, public-key)	Prevents communication content from being read by third parties.
Digital signature	Detects data tampering or impersonation of the sender, and makes it impossible for the sender to deny having sent the data afterward (**non-repudiation**).
Digital certificate	Verifies that the communication partner is authentic.
Multi-factor authentication	Prevents unauthorized logins.

Worked example: buying a product from an online shop

1. You access the site, HTTPS communication begins, and **encryption** prevents the content from being read by third parties.
2. The browser checks the **digital certificate** to confirm the destination is the genuine shopping site.
3. For account login, **multi-factor authentication** combining a password and SMS authentication prevents unauthorized logins.
4. When sending order details, a **digital signature** can also be used so that tampering during communication can be detected.

By combining multiple technologies in this way, various threats — **eavesdropping**, **tampering**, **impersonation** and **unauthorized login** — can be addressed simultaneously.

Key Terms

Term	Short definition
HTTPS	A way of carrying web communication securely: encryption, tamper detection and verification of the other party.
TLS handshake	The steps that establish the secure connection: certificate check and session-key sharing.
Public-key cryptography	Uses a pair of keys (public and private); shares a key safely.
Common-key cryptography	Uses session keys to exchange large amounts of data quickly.
Digital certificate	Verifies that the communication partner is authentic and matches the domain name.
Digital signature	Detects tampering and impersonation, and provides non-repudiation.
Non-repudiation	The sender cannot later deny having sent or signed the data.

Multi-factor authentication	Combining two or more of the three factors: knowledge, possession, biometric.
Certificate authority	The body that vouches that a site is genuine by issuing its certificate.

Lesson summary in 5 lines

1. HTTPS = HTTP over TLS — confidentiality, integrity and identity verification.
2. Handshake: digital certificate → session keys derived → then data exchanged.
3. Public-key shares keys safely; common-key exchanges data quickly.
4. MFA protects the account even if the password leaks — provided the factors are from different categories.
5. Encryption blocks reading, certificates prove identity, signatures detect tampering, MFA blocks unauthorized login.

Question Bank — Lesson 2-1

Part 1: Fill in the blanks

1. HTTP carried over a secured TLS connection is called .....
2. The steps that establish a secure TLS connection are called the .....
3. The type of cryptography used to exchange large amounts of session data quickly is .....
4. The technology that verifies that the communication partner is authentic is the .....
5. The technology that detects tampering and provides non-repudiation is the .....
6. Combining two or more of the three authentication factors is called .....
7. The three factors of authentication are ....., ... and .....
8. Public-key cryptography uses a ..... of keys: a ..... key and a ..... key.
9. TLS provides data in transit with ..... and .....
10. The property meaning the sender cannot later deny sending the data is .....
11. Public-key cryptography is used to ....., while common-key cryptography is used to .....
12. Four threats addressed by combining security technologies are ....., ..., ... and .....

Part 2: Choose the correct answer

1. HTTPS communication uses:

   (a) public-key cryptography only (b) common-key cryptography only (c) both, each in its own stage (d) no cryptography

2. Which of the following is **not** an example of multi-factor authentication?

   (a) password + smartphone notification (b) password + secret question (c) fingerprint + smart card (d) password + SMS authentication

3. Which of the following is **not** an appropriate description of a security technology?

   (a) Encryption prevents communication content from being read (b) Digital signatures improve communication speed
   (c) Digital certificates verify that the partner is authentic (d) Combining technologies addresses several threats at once

4. "Password + fingerprint authentication" is a combination of:

   (a) knowledge + possession (b) knowledge + biometric (c) biometric + possession (d) knowledge + knowledge

5. "Smart card + fingerprint authentication" is a combination of:

   (a) knowledge + possession (b) knowledge + biometric (c) possession + biometric (d) possession + possession

6. The most suitable technology for the threat "a user was directed to a fake site":

   (a) encryption (b) digital signature (c) digital certificate (d) MFA

7. The most suitable technology for the threat "communication content was intercepted by a third party":

   (a) encryption (b) digital signature (c) digital certificate (d) MFA

8. The most suitable technology for the threat "a password leaked and an unauthorized login occurred":

   (a) encryption (b) digital signature (c) digital certificate (d) MFA

9. The most suitable technology for the threat "data was altered during communication":

   (a) encryption (b) digital signature (c) digital certificate (d) MFA

10. The reason common-key cryptography is used for session data is:

    (a) it is always more secure than public-key (b) it exchanges large amounts of data quickly
    (c) it needs no keys at all (d) it removes the need for a certificate

11. In the TLS handshake, the session key is:

    (a) sent in plain text (b) derived at each side without the key itself being sent (c) written inside the certificate (d) sent by SMS

12. What does using HTTPS **not** guarantee?

    (a) the connection is encrypted (b) the server's identity is verified (c) the site's content is honest and trustworthy (d) data integrity in transit

13. A school is building a fee-payment portal. The most secure sign-in method is:

    (a) password only (b) password + a one-time code on the phone (c) secret question only (d) username only

14. The main role of public-key cryptography in TLS is:

    (a) encrypting all session data (b) authentication and safely sharing the session keys (c) compressing data (d) speeding up the network

Part 3: True (✓) or False (✗) — correct the false statements

1. HTTPS communication uses both public-key cryptography and common-key cryptography. ( )
2. HTTPS communication exchanges all data using public-key cryptography. ( )
3. Multi-factor authentication combines two or more of the three factors of authentication. ( )
4. An example of multi-factor authentication is setting two passwords. ( )
5. A digital certificate helps verify the server's identity and domain name. ( )
6. A digital signature increases communication speed. ( )
7. The presence of HTTPS means the site's content is trustworthy. ( )
8. An account stays relatively protected after a password leak if MFA is enabled. ( )
9. The session key is sent in plain text across the network during the handshake. ( )
10. Combined security technologies remove every threat completely. ( )

Part 4: Match each threat with the appropriate technology

Threat / requirement	Options
1) I want to prevent communication content from being read by third parties	(a) encryption (b) digital signature (c) digital certificate (d) multi-factor authentication
2) I want to verify that data has not been altered and came from the claimed sender	
3) I want to verify that the communication partner is authentic	
4) I want to reduce the risk of a login after a password leak	

Part 5: Identify the combination of authentication factors

Options: **(a)** knowledge + possession **(b)** knowledge + biometric **(c)** biometric + possession.

1. Password + one-time password.
2. Password + fingerprint authentication.
3. Password + SMS authentication.
4. Face recognition + smart card.

Part 6: Extended-response questions

1. **Explain why** public-key cryptography is not used to exchange all the session data.
2. **Explain why** "password + secret question" is not true multi-factor authentication.

3. **Explain why** an account stays protected by a second factor even if the password is leaked.
4. **State** three ordered steps by which a secure HTTPS connection is established.
5. **What is the difference** between a digital certificate and a digital signature in terms of function?
6. **Exam-style question [6 marks]:** Explain why TLS uses public-key mechanisms for authentication and safe key sharing, and then uses common-key cryptography to protect session data. Use the ideas of **security** and **speed**.
7. **In a new context:** A small online shop wants to secure both customer login and payment. Name two security technologies it must use, state where each one helps, and identify one threat that could still remain.

2-2 Network Security Design

Learning objectives

- Explain the roles of firewalls, VPNs, DMZs and endpoint controls in protecting a network.
- Explain why defense in depth gives stronger protection than relying on a single measure.
- Evaluate a network security design and justify the controls chosen for its assets and threats.

Key fact

Strong network security comes from **layering measures** — firewall, VPN, DMZ, endpoint protection — and from **verifying every access** (zero trust), not from a single barrier.

1. The Role of Firewalls

Firewall: a system installed at the entry/exit point of a network that **allows or denies communication based on rules set in advance**. It can sit at the network boundary, between parts of a network, or on a host machine.

Example: allow access to the web server, but deny direct external access to the database server.

2. VPN (Virtual Private Network)

VPN: a technology that creates an **encrypted virtual private line (tunnel)** over the Internet, allowing safe connection to a network from a remote location.

Main uses of VPN

1. **Remote work** — connecting safely to an organization's network from home or while away.
2. **Connecting branches** — connecting offices in different locations safely.

Good to know

Because communication content is encrypted when using a VPN, the risk of **eavesdropping** is reduced even on public Wi-Fi. But a VPN does **not** delete viruses or scan files — that is the job of endpoint controls.

3. DMZ (Demilitarized Zone)

DMZ: an area where servers exposed to the external network (web servers, mail servers, etc.) are placed **separately from the internal network**.

Benefit: by providing a DMZ, even if a public-facing server is attacked, damage to the **internal network** — which holds the confidential data — can be prevented.

Careful

A DMZ is **not** a system that exposes all servers to the outside, and it has nothing to do with improving connection **speed**. Its purpose is **separation**.

4. Defense in Depth

Defense in depth: the concept of **layering multiple security measures** so that, even if one measure is breached, the next can still protect the system.

Layer	Examples of measures
Layer 1: Network entry	Block unauthorized communication using a **firewall**.
Layer 2: Communication path	Encrypt communication using a **VPN**.
Layer 3: Server placement	Separate public-facing servers from the internal network using a **DMZ**.
Layer 4: Endpoints	Install antivirus software and keep the **OS updated**.

5. The Concept of Zero Trust

Zero trust: a security concept meaning the system does **not trust any communication**, including communication from within the organization's network, and **always verifies it**. Even for access from inside the organization, identity verification and access-permission checks are performed every time.

Why did this concept appear?

Conventional network security was designed mainly around protecting a **perimeter**, based on the premise that "inside the organization's network is safe, and outside is dangerous". However, with the spread of **cloud services** and **remote work**, the boundary between inside and outside has become blurred, and designs that protect only the perimeter have become insufficient.

Key Terms

Term	Short definition
Firewall	Allows or denies communication at a network's entry/exit point based on preset rules.
VPN	An encrypted virtual private line (tunnel) over the Internet for safe remote connection.
DMZ	A zone for public-facing servers, separated from the internal network.
Defense in depth	Layering multiple security measures so that one breach does not expose everything.
Zero trust	Verify every access; trust nothing automatically because of its location.
Perimeter	The traditional boundary assuming "inside is safe", blurred by cloud and remote work.
Endpoint	The user device itself, protected by antivirus software and OS updates.

Lesson summary in 5 lines

1. Firewall = allow or deny by preset rules, at the network entry/exit point.
2. VPN = an encrypted private tunnel over a public network, for remote work and branch links.
3. DMZ = separates public-facing servers from the internal network to limit breach damage.
4. Defense in depth = four layers: network entry, communication path, server placement, endpoints.
5. Zero trust = no automatic trust by location; verify identity and permissions every time.

Question Bank — Lesson 2-2

Part 1: Fill in the blanks

1. The system that allows or denies communication at a network's entry/exit point based on preset rules is the .....
2. The abbreviation describing an encrypted virtual private line over the Internet is .....
3. The three-letter abbreviation for the zone where externally exposed servers are placed is .....
4. The concept of layering multiple security measures is called .....
5. The security concept that does not trust any communication and always verifies it is .....

6. The traditional boundary assuming "inside is safe" is called the .....
7. The two main uses of a VPN are ..... and .....
8. The four layers of defense in depth are ....., ..., ... and .....
9. The two developments that blurred the boundary between inside and outside are ..... and .....
10. Endpoint protection includes installing ..... and keeping the ..... updated.

Part 2: Choose the correct answer

1. Which of the following is **not** an appropriate use of a VPN?

   (a) connecting safely from home to the organization's network (b) connecting offices in different locations
   (c) automatically deleting virus-infected files (d) encrypting communication on public Wi-Fi

2. The most appropriate reason for using a DMZ:

   (a) to improve connection speed (b) to expose all servers to the outside
   (c) to prevent damage to the internal network even if a public server is attacked (d) to detect and remove viruses

3. The most appropriate description of zero trust:

   (a) access from inside the network is safe so no check is needed (b) a firewall alone is sufficient
   (c) nothing is trusted automatically and every access is verified (d) only external access needs monitoring

4. "Install antivirus software and keep the OS updated" belongs to which layer?

   (a) network entry (b) communication path (c) server placement (d) endpoints

5. "Separate public-facing servers from the internal network" belongs to which layer?

   (a) network entry (b) communication path (c) server placement (d) endpoints

6. "Block unauthorized communication using a firewall" belongs to which layer?

   (a) network entry (b) communication path (c) server placement (d) endpoints

7. "Encrypt communication using a VPN" belongs to which layer?

   (a) network entry (b) communication path (c) server placement (d) endpoints

8. A firewall operates on the basis of:

   (a) the type of device only (b) rules set in advance (c) connection speed (d) number of users

9. Placing a public web server inside the internal network instead of a DMZ increases the risk of:

   (a) a slow website (b) an attacker reaching confidential internal data (c) higher cost (d) power failure

10. A hospital moves patient records to the cloud and allows access from home. The two most suitable measures are:

    (a) VPN + verifying every access (zero trust) (b) removing passwords (c) opening all ports (d) relying on the perimeter alone

11. The core idea of defense in depth is:

    (a) use one strongest technology (b) if one layer fails, other layers still reduce the risk (c) reduce cost (d) increase speed

12. Which of the following is **not** a possible location for a firewall?
    (a) at the network boundary (b) between parts of a network (c) on a host machine (d) inside the network cable itself

Part 3: True (✓) or False (✗) — correct the false statements

1. A firewall allows or denies communication based on rules set in advance. ( )
2. Using a VPN can reduce the risk of eavesdropping even on public Wi-Fi. ( )
3. A DMZ is a system that exposes all servers to the outside. ( )
4. Defense in depth is the concept of layering multiple security measures. ( )
5. In zero trust, every device inside the network is trusted automatically. ( )
6. A VPN automatically deletes virus-infected files. ( )
7. Protecting only the perimeter has become insufficient because of cloud services and remote work. ( )
8. A firewall can be placed between parts of an internal network, not only at its boundary. ( )

Part 4: Match each description with the correct term

Description	Options
1) A technology creating an encrypted virtual private line over the Internet for safe remote connection	(a) firewall (b) VPN (c) DMZ (d) defense in depth
2) An area where servers exposed to the outside are placed separately from the internal network	
3) A system that allows or denies communication based on rules set in advance	
4) Layering multiple security measures	

Part 5: Extended-response questions

1. **Explain why** it is safer to place a public web server in a DMZ rather than inside the internal network.
2. **Explain why** protecting only the perimeter is no longer sufficient today.
3. **Explain why** the risk of eavesdropping is reduced when a VPN is used on public Wi-Fi.
4. **What is the difference** between a firewall and a VPN in terms of function?
5. **Exam-style question [6 marks]:** Explain why layering several security measures (defense in depth) protects an organization better than relying on a firewall alone. Refer to what happens when one measure is breached.

6. **In a new context:** A company has a public website, employees working from home, and a confidential customer database. Match each asset to the most suitable protection layer, then name one layer whose failure would be most damaging and explain why it is not enough on its own.

2-3 Incident Response and Risk Management

Learning objectives

- Explain the six stages of incident response and the purpose of each.
- Use **impact** and **likelihood** to prioritise risks.
- Design a justified response to a security incident and link response actions to preventive controls.

Key fact

Incident response follows **six ordered stages**, and risk assessment prioritises risks by **impact × likelihood** — so an organization acts in the right order and on the right risks first.

1. What is a Security Incident

Security incident: a situation in which actual damage occurs due to an information security problem.

Type	Description
Information leak	Personal information or confidential information is leaked to the outside.
Data tampering	Data within a system is altered without authorization.
Service outage	A service becomes unavailable due to attacks on the server, etc.

Careful

Updating software to add new features is **not** a security incident — it is normal operation.

2. The Flow of Incident Response — Six Stages

Stage	Description
① Preparation	Establish response procedures and structures **in advance**, in preparation for incidents.
② Detection	Discover and confirm that an incident has occurred.

③ Containment	Limit the scope of impact so that **damage does not spread further**.
④ Eradication	Remove the cause of the incident (e.g. remove malware and fix the exploited weakness).
⑤ Recovery	Return systems and services to their normal state (often restoring from a clean backup).
⑥ Prevention of recurrence	Analyze the cause and take measures so that the same incident does not occur again.

Why containment before eradication?

Because the first goal is to **stop the damage spreading** before dealing with the cause. Likewise, if **recovery is performed without identifying the cause**, the same incident may occur again — the malware or the weakness would still be there.

3. The Concept of Risk Assessment

Risk: the possibility of an information security problem occurring in the future, and its impact.

The rule of this lesson

Risk size = Impact × Likelihood

- **Impact** — how much damage occurs if the risk actually materializes.
- **Likelihood** — how high the probability is that the risk will actually materialize.

Risks with both **high impact and high likelihood** should be addressed first. Since it is difficult to address all risks at the same time, it is important to **set priorities** and take measures systematically.

Key Terms

Term	Short definition
Security incident	A situation in which actual damage occurs due to an information security problem.
Containment	Limiting the scope of impact so damage does not spread.
Eradication	Removing the cause of the incident, such as malware.
Recovery	Returning systems and services to their normal state.
Prevention of recurrence	Analyzing the cause and taking measures so it does not happen again.
Impact	How much damage occurs if a risk materializes.

Likelihood	How probable it is that a risk will materialize.

Lesson summary in 4 lines

1. A security incident causes actual damage: information leak, data tampering, or service outage.
2. Six stages: preparation → detection → containment → eradication → recovery → prevention of recurrence.
3. Order matters: recovering before finding the cause lets the same incident happen again.
4. Priority goes to risks with high impact and high likelihood.

Question Bank — Lesson 2-3

Part 1: Fill in the blanks

1. A situation in which actual damage occurs due to an information security problem is a .....
2. The six stages of incident response in order are ..... → ..... → ..... → ..... → ..... → .....
3. The two factors that determine the size of a risk are ..... and .....
4. The stage that limits the scope of impact so damage does not spread is .....
5. The stage that removes the cause of the incident is .....
6. The final stage of incident response is .....
7. Altering data within a system without authorization is called .....
8. How much damage occurs if a risk materializes is called ....., and how probable it is is called .....
9. Establishing response procedures and structures in advance happens in the ..... stage.
10. The three typical types of security incident are ....., ... and .....

Part 2: Choose the correct answer

1. Which of the following is **not** an appropriate example of a security incident?
   (a) data encrypted by ransomware (b) customer information leaked through unauthorized access
   (c) updating software to add new features (d) a web service stopped by an attack on the server
2. The most appropriate description of risk assessment:
   (a) only high-impact risks need addressing (b) only high-likelihood risks need addressing
   (c) risks with high impact and high likelihood are addressed first (d) all risks are addressed at the same time

3. The correct order of the response flow:
   (a) detection → eradication → containment → recovery (b) preparation → detection → containment → eradication → recovery → prevention of recurrence
   (c) detection → recovery → containment → prevention (d) containment → detection → eradication → preparation
4. "Disconnecting a malware-infected computer from the network" belongs to which stage?
   (a) preparation (b) containment (c) eradication (d) prevention of recurrence
5. "Analyzing the cause and taking measures to stop it happening again" belongs to which stage?
   (a) preparation (b) containment (c) eradication (d) prevention of recurrence
6. A risk with (impact: large, likelihood: high) has a priority that is:
   (a) the lowest (b) the highest (c) always medium (d) impossible to determine
7. Why must containment come before eradication?
   (a) it is cheaper (b) to stop the damage spreading first (c) it is faster to perform (d) it needs no team
8. The danger of starting recovery before removing the cause is:
   (a) losing the backups (b) the malware or weakness remains and the incident repeats (c) a slower network (d) higher cost only
9. The reason organizations set priorities among risks is:
   (a) some risks are not real (b) no team can fix everything at once (c) to save electricity (d) to reduce staff numbers
10. An online shop has just detected a customer-data leak. The next two stages are:
    (a) preparation then detection (b) containment then eradication (c) recovery then containment (d) prevention then preparation
11. "Restoring systems from a clean backup" belongs to which stage?
    (a) containment (b) eradication (c) recovery (d) detection
12. Which of these is a **preventive** control that makes recovery possible at all?
    (a) regular clean backups (b) faster Internet (c) more staff (d) a larger screen

Part 3: True (✓) or False (✗) — correct the false statements

1. A security incident is a situation in which actual damage occurs due to an information security problem. ( )
2. In incident response, it is important to stop the damage spreading before removing the cause. ( )
3. The size of a risk can be determined by impact alone. ( )
4. The final stage of incident response is prevention of recurrence. ( )
5. If recovery is performed without identifying the cause, the same incident may occur again. ( )
6. Updating software to add a new feature is a security incident. ( )
7. The preparation stage must be carried out before an incident occurs. ( )
8. A risk with small impact and low likelihood has the lowest priority. ( )

Part 4: Match each action with the correct stage

Action	Options
1) Establishing response procedures in advance, ready for incidents	(a) preparation (b) containment (c) eradication (d) prevention of recurrence
2) Disconnecting a malware-infected computer from the network	
3) Removing the malware infection and fixing the weakness	
4) Analyzing the cause and taking measures to ensure it does not repeat	

Part 5: Rank the risks by priority

Use the rule (impact × likelihood) to rank the following risks. If two are equal or the information is not enough to rank them, say so and explain.

1. Impact: large · Likelihood: high
2. Impact: small · Likelihood: high
3. Impact: large · Likelihood: low
4. Impact: small · Likelihood: low

Part 6: Extended-response questions

1. **Explain why** containment must come before eradication.
2. **Explain why** impact alone is not enough to determine a risk's priority.
3. **Explain why** performing recovery before eradication is dangerous.
4. **Exam-style question [6 marks]:** Explain the importance of following the six stages of incident response in order, using containment, eradication and recovery as your example, and explain what can go wrong if the order is not followed.
5. **In a new context:** A school's student-records system is hit by ransomware: the files are encrypted and staff can no longer log in. State the stages still to be carried out and what each one means in this specific incident. Then compare the risk of "another ransomware attack" with the risk of "a short power cut" in terms of impact and likelihood, and say which should be addressed first.

Chapter Test

Chapter 2 — Cyber Security

Instructions

Time: 1 hour · Total marks: 40 · Answer all questions.

Question 1: Choose the correct answer [10 marks]

1. The type of cryptography used to protect session data after the handshake is:
   (a) public-key (b) common-key (c) none (d) the digital signature
2. "Password + secret question" represents:
   (a) valid multi-factor authentication (b) two factors from the same knowledge category (c) knowledge + possession (d) biometric + possession
3. The purpose of a DMZ is:
   (a) to speed up the network (b) to separate public servers from the internal network (c) to delete viruses (d) to encrypt passwords
4. "Install antivirus software and keep the OS updated" is which layer?
   (a) network entry (b) communication path (c) server placement (d) endpoints
5. Zero trust means:
   (a) trusting every internal device (b) verifying every access (c) blocking the Internet (d) relying on the firewall alone
6. The correct stage order is:
   (a) containment → detection → eradication (b) detection → containment → eradication → recovery (c) recovery → containment → detection (d) eradication → containment → detection
7. Risk size is estimated by:
   (a) impact only (b) likelihood only (c) impact × likelihood (d) number of devices
8. The technology that provides non-repudiation is the:
   (a) digital certificate (b) digital signature (c) firewall (d) VPN
9. Which of the following is **not** a security incident?
   (a) a data leak (b) data tampering (c) a planned software update (d) a service outage caused by an attack
10. The function of a digital certificate is:
    (a) to speed up the connection (b) to verify the server's identity and domain (c) to delete viruses (d) to create a backup

Question 2: Fill in the blanks [8 marks]

1. The steps that establish a secure TLS connection are called the .....
2. The three factors of authentication are knowledge, ... and .....
3. The abbreviation for an encrypted private line over a public network is .....
4. Layering multiple security measures is called .....
5. The traditional boundary assuming "inside is safe" is the .....
6. The stage that limits the spread of damage is .....
7. How much damage occurs if a risk materializes is called .....
8. The property preventing a sender from denying they sent the data is .....

Question 3: True (✓) or False (✗) — correct the false statements [6 marks]

1. HTTPS exchanges all data using public-key cryptography. ( )
2. A VPN deletes virus-infected files. ( )
3. Defense in depth is the layering of security measures. ( )
4. Risk size can be determined by impact alone. ( )
5. Multi-factor authentication reduces the risk of unauthorized login after a password leak. ( )
6. The presence of HTTPS guarantees the site's content is honest. ( )

Question 4: Match the two columns [4 marks]

(A)	(B)
1) Allows or denies communication based on rules	(a) DMZ (b) firewall (c) digital signature (d) VPN
2) An encrypted private line over a public network	
3) Separates public servers from the internal network	
4) Detects tampering and supports non-repudiation	

Question 5: Extended response [12 marks]

1. **[4 marks]** Explain why TLS uses two different types of cryptography in a single connection.
2. **[4 marks]** Explain why defense in depth is stronger than relying on a firewall alone.
3. **[4 marks]** Put the response stages for a ransomware incident in order, and explain the danger of starting recovery before eradication.

Model Answers

Chapter 2 question banks and chapter test

Lesson 2-1 — Answers

Part 1: Fill in the blanks

1) HTTPS. **2)** TLS handshake. **3)** Common-key cryptography. **4)** Digital certificate. **5)** Digital signature. **6)** Multi-factor authentication. **7)** Knowledge — possession — biometric. **8)** Pair — public — private. **9)** Confidentiality — integrity. **10)** Non-repudiation. **11)** Share keys safely — exchange large amounts of data quickly. **12)** Eavesdropping — tampering — impersonation — unauthorized login.

Part 2: Multiple choice

1) c **2)** b **3)** b **4)** b **5)** c **6)** c **7)** a **8)** d **9)** b **10)** b **11)** b **12)** c **13)** b **14)** b

Part 3: True / False

1) ✓ **2)** ✗ — public-key cryptography shares the keys safely, then **common-key cryptography** carries the session data because it is faster. **3)** ✓ **4)** ✗ — two passwords are both from the **knowledge** factor, so this is not multi-factor authentication. **5)** ✓ **6)** ✗ — a digital signature detects tampering and provides non-repudiation; it has nothing to do with speed.

7) ✗ — HTTPS secures the **connection** only; it says nothing about whether the content is trustworthy. **8)** ✓ **9)** ✗ — session keys are **derived at each side** without the key itself being sent. **10)** ✗ — they reduce the threats; they do not remove them **completely**.

Parts 4 and 5

Part 4: **1)** a **2)** b **3)** c **4)** d

Part 5: **1)** a **2)** b **3)** a **4)** c

Part 6: Extended response

1) Because public-key operations are comparatively **slow** and costly; they are used for authentication and safe key sharing only, after which common-key cryptography carries the data quickly and efficiently.

2) Because both factors come from the **knowledge** category — someone who obtained the password can often guess or obtain the secret answer too. Multi-factor authentication requires factors from **different categories**.

3) Because logging in also needs an **independent second factor** that the user possesses (a code from a device or app), and an attacker who stole only the password cannot supply it.

4) (1) The server sends its digital certificate and the browser checks its validity and that it matches the site name. (2) In the same handshake the two sides agree on shared secrets and derive session keys. (3) Once the handshake is complete, session data is protected with common-key cryptography and integrity mechanisms.

5) A **digital certificate** proves the **server's identity** and its link to the domain name before communication. A **digital signature** proves the **integrity of a specific message and the identity of its signer**, and supports non-repudiation.

6) Answer points: **Security** — public-key mechanisms let the browser verify the server through its certificate and let both sides agree on a shared secret without sending the key across the network, so an eavesdropper cannot extract it. **Speed** — public-key operations are relatively slow and unsuited to large volumes of data; once the session keys are derived, common-key cryptography is used because it is fast and light. The result: security when starting the connection, and speed when carrying the data.

7) Sample: (1) **HTTPS/TLS with a digital certificate** — encrypts payment and order details and proves the shop's identity to the customer. (2) **Multi-factor authentication** at login — reduces the risk of account takeover if the password leaks. A threat that could remain: phishing that tricks the customer into entering

details on a fake site, or a breach of the shop's own database.

Lesson 2-2 — Answers

Part 1: Fill in the blanks

1) Firewall. **2)** VPN. **3)** DMZ. **4)** Defense in depth. **5)** Zero trust. **6)** Perimeter. **7)** Remote work — connecting branches. **8)** Network entry — communication path — server placement — endpoints. **9)** Cloud services — remote work. **10)** Antivirus software — OS.

Part 2: Multiple choice

1) c **2)** c **3)** c **4)** d **5)** c **6)** a **7)** b **8)** b **9)** b **10)** a **11)** b **12)** d

Part 3: True / False

1) ✓ **2)** ✓ **3)** ✗ — a DMZ **separates** public-facing servers from the internal network; it does not expose all servers. **4)** ✓ **5)** ✗ — in zero trust **nothing is trusted automatically** because of its location, and every access is verified. **6)** ✗ — a VPN only encrypts the connection; deleting viruses is the job of endpoint controls. **7)** ✓ **8)** ✓

Part 4: Matching

1) b **2)** c **3)** a **4)** d

Part 5: Extended response

1) Because a public server is **exposed to the Internet** and more likely to be attacked; placing it in a DMZ separates it from the internal network, so a successful attack does not give the attacker direct access to confidential data.

2) Because **cloud services and remote work blurred the boundary** between inside and outside the network, so a user's location is no longer sufficient evidence that they can be trusted.

3) Because a VPN **encrypts the communication content** through a secure tunnel, so anyone eavesdropping on the public network cannot read the data passing through.

4) A **firewall** controls **who may enter or leave** the network according to rules (network-entry layer). A **VPN** protects the **content of the communication while it travels** over a public network by encrypting it (communication-path layer).

5) Answer points: relying on a firewall alone creates a **single point of failure** — if an attacker gets past it, or its rules are misconfigured, everything behind it is exposed. Layering assigns a control to each kind of threat: firewall at the entry, VPN on the path, DMZ for server placement, endpoint controls on each device. If one layer is breached, the remaining layers reduce the chance of a full compromise and **limit the damage**, so a single breach does not expose the whole system.

6) Sample: public website → server placement (DMZ), main threat being an attack on the public server. Remote employees → communication path (VPN), main threat being eavesdropping on public networks. Customer database → network entry and endpoints, main threat being unauthorized access. The layer whose failure hurts most is network entry (the firewall) — but it alone is not enough, because it does not protect data while it travels nor a device that has been infected with malware.

Lesson 2-3 — Answers

Part 1: Fill in the blanks

1) Security incident. **2)** Preparation → detection → containment → eradication → recovery → prevention of recurrence. **3)** Impact — likelihood. **4)** Containment. **5)** Eradication. **6)** Prevention of recurrence. **7)** Data tampering. **8)** Impact — likelihood. **9)** Preparation. **10)** Information leak — data tampering — service outage.

Part 2: Multiple choice

1) c **2)** c **3)** b **4)** b **5)** d **6)** b **7)** b **8)** b **9)** b **10)** b **11)** c **12)** a

Part 3: True / False

1) ✓ **2)** ✓ **3)** ✗ — risk size is determined by **impact and likelihood together**. **4)** ✓ **5)** ✓ **6)** ✗ — a planned update is **normal operation**, not a security incident. **7)** ✓ **8)** ✓

Parts 4 and 5

Part 4: **1)** a **2)** b **3)** c **4)** d

Part 5: The highest priority is risk **1** (large impact × high likelihood) and the lowest is risk **4** (small × low). Risks **2** and **3** sit close together, and the words alone are not enough to rank them; the order depends on the matrix scores, the context and the controls available.

Part 6: Extended response

1) Because the first goal is to **stop the damage spreading** and limit the scope of impact. If the team works on removing the cause first, the damage may reach other systems in the meantime.

2) Because a risk with a large impact but a very low likelihood may be less urgent than a moderate risk that happens often; that is why risk size is estimated as **impact × likelihood**.

3) Because the **cause has not been removed**: the malware or the exploited weakness is still present, so the restored system can be compromised again immediately and the same incident recurs.

4) Answer points: the ordered stages organise the work under pressure and prevent skipping ahead. **Containment** stops the spread first; then **eradication** removes the malware and fixes the weakness; then **recovery** restores service from a clean backup. If the order is not followed — for example recovering before eradication — the malware or weakness remains, the restored system is compromised again, and the team must return to containment and eradication, losing time and increasing damage.

5) Sample: **detection** has already happened. Still to be carried out: **containment** (disconnect the infected machines and servers from the network so the encryption stops spreading), **eradication** (remove the ransomware and fix the weakness it entered through), **recovery** (restore the student records from a clean backup and reopen the accounts), and **prevention of recurrence** (analyse the cause, set up regular backups and train staff). Comparison: another ransomware attack has a large impact and, after the first attack succeeded, a high likelihood → higher priority; a short power cut has a relatively small impact → lower priority.

Chapter 2 Test — Answers

Question 1

1) b **2)** b **3)** b **4)** d **5)** b **6)** b **7)** c **8)** b **9)** c **10)** b

Question 2

1) TLS handshake. **2)** Possession — biometric. **3)** VPN. **4)** Defense in depth. **5)** Perimeter. **6)** Containment. **7)** Impact. **8)** Non-repudiation.

Question 3

1) ✗ — session data is protected with **common-key** cryptography. **2)** ✗ — a VPN encrypts the connection; it does not delete viruses. **3)** ✓ **4)** ✗ — by impact **and likelihood together**. **5)** ✓ **6)** ✗ — it secures the connection only and says nothing about the honesty of the content.

Question 4

1) b **2)** d **3)** a **4)** c

Question 5

1) Because each type has a different job: public-key cryptography solves **authentication and safe key sharing** without sending the secret across the network, but it is slow; common-key cryptography is **fast and efficient**, so it suits the large volume of session data once the keys exist.

2) Because a firewall alone is a **single point of failure**: if an attacker passes it, everything behind it is exposed. Multiple layers reduce the chance of a breach and limit its damage, so one breach is not enough to compromise the whole system.

3) Order: preparation (beforehand) → detection → containment (isolate the infected machines) →

eradication (remove the ransomware and fix the weakness) → recovery (restore from a clean backup) → prevention of recurrence. The danger of recovering before eradication is that the **malware or the weakness is still present**, so the restored data is encrypted again and the team must return to containment.

Chapter 3

Web Applications

This chapter opens up the services you use every day. First, what a web application is made of — its **three tiers** (3-1). Then how those tiers actually talk to each other over the network — **requests, responses and APIs** (3-2). Finally, what the tier you can see is built from — **HTML, CSS and JavaScript** (3-3).

3-1 The Overall Structure of Web Applications

Learning objectives

- Explain what a web application is and describe the roles of its three tiers: frontend, backend, and database.
- Trace how the three tiers cooperate to turn a user's action into a result, using familiar services as examples.

Key fact

A web application is built from three tiers — **frontend, backend, and database** — that cooperate to turn a user's action into a result.

1. What is a Web Application?

Web application: an application used through a web browser. It can be used as long as you have a browser, **without needing to install dedicated software**.

Examples: YouTube, Amazon, Gmail, Google Maps.

2. The Three Tiers of a Web Application

Tier	Role	Examples
Frontend	The screen component that users see directly. It runs on the **browser** and accepts user input.	Search screen, product listing pages, input forms
Backend	The **server-side** processing that users do not see. It processes data and makes decisions.	Searching for products matching criteria, login authentication

Database	A system that organizes, stores, and manages data. It retrieves data when needed and records new data.	Product information, user information, order history

Careful — common mistakes

The backend runs **on the server, not on the browser**. And a web application does **not** operate with the frontend alone — all three tiers are needed.

3. How the Three Tiers Cooperate

Example: searching for a product on an online shopping site

1. The **frontend** receives the search keywords entered by the user.
2. The frontend sends the search keywords to the **backend**.
3. The backend searches the **database** for products that match the criteria.
4. The database returns the matching product data to the backend.
5. The backend organizes the search results and returns them to the frontend.
6. The frontend displays the search results on the user's screen.

A rule that answers most questions

The frontend **shows and collects**; the backend **decides and processes**; the database **stores and retrieves**.

4. Familiar Web Application Configurations

Service	Frontend (display and interaction)	Backend (processing and control)	Database (storage and management)
Video sharing site	Display of playback and search screens; reception of user operations	Selection of recommended videos; aggregation of view counts	Storage of video data, user information, viewing history
SNS	Display of timelines and post screens; sending of input content	Determining the audience for posts; control of push notifications	Storage of post data, follow relationships, messages
E-commerce site	Display of product listings and cart screens; reception of order operations	Stock checking; execution of payment systems	Storage of product information, order history, customer information

Every service uses the **same three tiers**; what changes from one service to the next is only **what each tier does**.

Key Terms

Term	Short definition
Web application	An application used through a web browser, with no dedicated software to install.
Frontend	The screen users see and interact with; runs on the browser.
Backend	The hidden server-side processing that handles data and decisions.
Database	Where data is organized, stored, retrieved and managed.
Three-tier architecture	Frontend + backend + database cooperating to serve a user's action.

Lesson summary in 4 lines

1. A web application runs in a browser with nothing to install.
2. Three tiers: frontend (screen), backend (server processing), database (data).
3. Flow: input → frontend → backend → database → back up the chain → display.
4. All familiar services (video, SNS, e-commerce) use the same three tiers.

Question Bank — Lesson 3-1

Part 1: Fill in the blanks

1. An application used through a web browser without installing dedicated software is a .....
2. The screen component that users see directly is the .....
3. The part responsible for server-side processing that users do not see is the .....
4. A system that organizes, stores, and manages data is a .....
5. The three tiers of a web application are ....., ... and .....
6. The frontend runs on the ....., while the backend runs on the .....
7. The structure formed by the three tiers cooperating is called the .....
8. On an e-commerce site, stock checking is handled by the ....., while order history is kept in the .....

Part 2: Choose the correct answer

1. Which tier searches the data for products matching the search keywords?
   (a) frontend (b) backend (c) database (d) browser

2. Which of the following is **not** a web application?
   (a) Gmail (b) YouTube (c) Google Maps (d) the operating system of a laptop
3. The correct order of the search flow is:
   (a) frontend → database → backend → frontend (b) frontend → backend → database → backend → frontend
   (c) backend → frontend → database (d) database → frontend → backend
4. The tier that "shows and collects" is the:
   (a) frontend (b) backend (c) database (d) network
5. Selecting recommended videos on a video site is the job of the:
   (a) frontend (b) backend (c) database (d) browser
6. Storing follow relationships on an SNS is the job of the:
   (a) frontend (b) backend (c) database (d) frontend and backend together
7. Displaying the cart screen is the job of the:
   (a) frontend (b) backend (c) database (d) payment system
8. A booking page opens normally, but no free time slots appear. The tier that is clearly working is:
   (a) the frontend (b) the backend (c) the database (d) none of them
9. What advantage does a web application have over installed software?
   (a) it works without a browser (b) it needs no dedicated software installed (c) it needs no server (d) it stores no data
10. Which statement about the three tiers is correct?
    (a) the backend runs on the browser (b) the frontend alone can run the application
    (c) each tier has a distinct role and all three are needed (d) the database displays the screen

Part 3: True (✓) or False (✗) — correct the false statements

1. The frontend is the screen component that users see directly. ( )
2. The backend is the part that runs on the browser. ( )
3. A database is a system that organizes, stores, and manages data. ( )
4. A web application operates with the frontend alone. ( )
5. A web application requires dedicated software to be installed first. ( )
6. Video sites, SNS and e-commerce sites all use the same three-tier structure. ( )

Part 4: Match each description with the correct tier

Description	Options
1) The part responsible for server-side processing that users do not see	(a) frontend (b) backend (c) database
2) The screen component that users interact with directly	

3) A system that organizes, stores, and manages data	

Part 5: Classify by tier

For each item, state which tier of an e-commerce site it belongs to: **(a)** frontend **(b)** backend **(c)** database.

1. Product listing page
2. Stock checking processing
3. Storage of customer information
4. Cart screen
5. Payment processing
6. Storage of order history

Part 6: Extended-response questions

1. **Explain why** a web application cannot work with the frontend alone.
2. **Explain why** the same three-tier structure appears in services as different as a video site and an online shop.
3. **Exam-style question [6 marks]:** Explain how the three tiers of a web application cooperate when a user posts a photo on a social media app. Refer to the role of the frontend, the backend, and the database.
4. **Diagnose a fault:** A clinic booking page opens normally, but no free slots appear on screen. Which tier is clearly working, and which one has probably failed? Explain your reasoning.
5. **In a new context:** A weather app lets users type a city and see the forecast. Name which tier does each job — taking the city name, looking up the forecast data, and storing past forecasts — and identify one job the frontend cannot do on its own.

3-2 Web Application Communication Methods

Learning objectives

- Explain the client and server model and the difference between HTTP and HTTPS.
- Describe how HTTP requests and responses work, and explain the role of an API in exchanging data.

> **Key fact**
>
> Web applications work by a **client sending requests** and a **server returning responses**, using protocols (HTTP/HTTPS) and often APIs that exchange data in formats like JSON.

1. Client and Server

- **Client:** the side that **requests** data or processing from the server. Web browsers and smartphone apps fall into this category.
- **Server:** the side that **receives requests** from clients, processes them, and **returns responses**.

A web application operates by the client sending a **request** and the server returning a **response**.

2. HTTP and HTTPS

Protocol	Description
HTTP (HyperText Transfer Protocol)	A communication protocol for exchanging data between clients (browsers and apps) and servers.
HTTPS (HTTP Secure)	A communication protocol that adds **TLS encryption** to HTTP. Because the content is encrypted, the risk of it being read by third parties is reduced.

Websites whose URLs begin with **https://** use HTTPS communication. A login page should always use HTTPS, because the password would otherwise travel in a form third parties could read.

3. HTTP Requests and Responses

Requests sent from the client to the server include an **HTTP method** that indicates what kind of operation is desired.

Method	Role	Examples
GET	Retrieve data **from** the server	Displaying a web page, retrieving search results
POST	Send data **to** the server	Sending login information, submitting form contents

Responses returned from the server include a number indicating the result of processing, called a **status code**.

Status code	Meaning
200	Success — the request was processed successfully
404	Page not found — the specified URL does not exist

500	Server error — a problem occurred on the server side

> **Which side had the problem?**
>
> **404** means the address the client asked for does not exist — the page is missing. **500** means the fault is on the **server side**, not with what the user typed.

4. API (Application Programming Interface)

API: a system for exchanging data between **different pieces of software**. In web applications, the frontend often sends requests to the backend **through an API** and receives data back.

Data exchanged through an API is often described in a format called **JSON (JavaScript Object Notation)** — a data format that is both **easy for humans to read** and **easy for computers to process**.

Key Terms

Term	Short definition
Client	The side that requests data or processing (browser, smartphone app).
Server	The side that processes requests and returns responses.
HTTP	The protocol for exchanging data between clients and servers.
HTTPS	HTTP with TLS encryption added.
HTTP method	Says what is wanted: GET retrieves, POST sends.
Status code	Reports the result: 200 success, 404 not found, 500 server error.
API	A system for exchanging data between different pieces of software.
JSON	A data format easy for humans to read and computers to process.

Lesson summary in 4 lines

1. Client requests, server responds — that is how every web application communicates.
2. HTTP is the protocol; HTTPS is HTTP plus TLS encryption.
3. GET retrieves data, POST sends data; 200 success, 404 not found, 500 server error.
4. APIs exchange data between software, often in JSON format.

Question Bank — Lesson 3-2

Part 1: Fill in the blanks

1. The side that requests data or processing from the server is the .....
2. The side that receives requests, processes them and returns responses is the .....
3. The communication protocol for exchanging data between browsers and servers is .....
4. The protocol that adds TLS encryption to HTTP is .....
5. The HTTP method for retrieving data from the server is ....., and for sending data is .....
6. The number in a response indicating the result of processing is the .....
7. Status code ..... means success, ... means page not found, and ..... means server error.
8. A system for exchanging data between different pieces of software is an .....
9. The data format that is easy for both humans to read and computers to process is .....
10. URLs that begin with ..... use encrypted communication.

Part 2: Choose the correct answer

1. Which combination of status code and meaning is **not** appropriate?
   (a) 200 — the request was processed successfully (b) 404 — page not found
   (c) 500 — the request was processed successfully (d) 500 — a problem occurred on the server side
2. The GET method is used to:
   (a) send data to the server (b) retrieve data from the server (c) encrypt the connection (d) delete a page
3. Submitting a login form uses which method?
   (a) GET (b) POST (c) JSON (d) 200
4. A web browser is an example of a:
   (a) server (b) client (c) database (d) protocol
5. The main difference between HTTP and HTTPS is:
   (a) speed (b) added TLS encryption (c) the file format (d) the number of methods
6. A browser receives status code 404. This means:
   (a) the server crashed (b) the requested page does not exist (c) the request succeeded (d) the connection is not encrypted
7. Why should a login page use HTTPS rather than plain HTTP?
   (a) it loads faster (b) the password would otherwise be readable by third parties (c) it uses fewer methods (d) it avoids status codes
8. In a web application, the frontend usually gets its data from the backend through:
   (a) a database driver (b) an API (c) a status code (d) CSS

9. JSON is best described as:
   (a) a programming language (b) a data format (c) a protocol (d) a server
10. Status code 500 indicates the problem is:
    (a) on the client side (b) on the server side (c) in the URL spelling (d) in the browser version

Part 3: True (✓) or False (✗) — correct the false statements

1. The client requests data or processing, and the server returns the response. ( )
2. HTTPS is a communication protocol that adds encryption to HTTP. ( )
3. The GET method is for sending data to the server. ( )
4. Status code 404 indicates that the page is not found. ( )
5. An API is a system for exchanging data between different pieces of software. ( )
6. JSON can only be read by computers and is impossible for humans to read. ( )

Part 4: Match each description with the correct term

Description	Options
1) A communication protocol for exchanging data between web browsers and servers	(a) HTTP (b) API (c) HTTPS
2) A system for exchanging data between different pieces of software	
3) A communication protocol that adds encryption to HTTP	

Part 5: Extended-response questions

1. **Explain why** a login page must use HTTPS rather than plain HTTP.
2. **Explain the difference** between status codes 404 and 500 in terms of where the problem lies.
3. **Explain why** GET and POST are not interchangeable.
4. **Exam-style question [6 marks]:** Explain what happens, step by step, when a browser requests a web page and the server responds. Refer to: client, request, HTTP method, response, status code.
5. **In a new context:** A weather app fetches forecast data from another company's service. Explain what an API is doing here, what format the data is likely to arrive in, and what the app should display if it receives a 500 status code.

3-3 Fundamentals of Frontend Technology

Learning objectives

- Explain the distinct roles of HTML, CSS, and JavaScript in building a web page.
- Describe how semantic HTML, responsive design, and frameworks improve a modern frontend.

Key fact

A web page is built from **HTML (structure)**, **CSS (appearance)**, and **JavaScript (behavior)**; a modern frontend adds semantic HTML, responsive design, and frameworks.

1. The Roles of HTML, CSS, and JavaScript

Technology	Role	Analogy
HTML	Defines the **structure** (skeleton) of a web page. Describes elements such as headings, paragraphs, images, and links.	The frame of a building
CSS	Specifies the **appearance** of a web page (colors, layout, size, fonts).	The interior and exterior of a building
JavaScript	Adds **behavior and interactivity**. Activates responses when buttons are pressed and updates only part of the screen.	The electrical and plumbing systems

These three technologies each have **independent roles**, and a web page is created using all of them in combination.

Careful — a very common mistake

CSS specifies **appearance**. Adding behavior is **JavaScript**, not CSS.

2. Semantic HTML

Semantic HTML: the concept of describing each part of a web page using element names (tags) that **indicate their meaning**.

Example: use **<header>** at the top of the page, **<nav>** for navigation, **<main>** for the body, and **<footer>** at the bottom.

Benefits of semantic HTML

1. **Improved accessibility** — screen reader software can correctly understand the structure of the page, so information is easier to convey to users with visual impairments.
2. **Improved SEO (Search Engine Optimization)** — search engines can more easily understand the content correctly, making it more likely to be displayed appropriately in search results.

3. Responsive Design

Responsive design: a design concept in which the layout is **automatically adjusted** according to different screen sizes such as PCs, smartphones, and tablets. With a single web page, a display that is easy to view from any device can be achieved.

Websites are frequently accessed from smartphones, so support for responsive design is widely required. Against this backdrop, the **mobile-first** concept — prioritizing small screens from the design stage — has also become widespread.

4. Frameworks

Framework: a structure that provides **commonly used functions and components in advance**, in order to make web application development more efficient. By using a framework, developers do not need to write all code from scratch.

Framework	Characteristics
React	Developed by Meta (formerly Facebook). Can efficiently update only part of the screen; suited to large-scale web applications.
Vue	Has a simple structure and allows web applications to be built incrementally from small features.
Next.js	In addition to React's features, includes mechanisms to speed up page display.

Key Terms

Term	Short definition
HTML	Defines the structure (skeleton) of a web page.
CSS	Specifies the appearance: colors, layout, size, fonts.
JavaScript	Adds behavior and interactivity to a page.
Semantic HTML	Using tags whose names indicate the meaning of each part.
Accessibility	Making information usable by everyone, including screen reader users.
SEO	Helping search engines understand a page so it appears appropriately in results.

Responsive design	Layout adapts automatically to the screen size.
Mobile-first	Designing for small screens first.
Framework	Ready-made functions and components for efficient development.

Lesson summary in 4 lines

1. HTML structures, CSS styles, JavaScript adds behavior — three independent roles.
2. Semantic HTML improves accessibility and SEO.
3. Responsive design adapts one page to every screen size; mobile-first starts small.
4. Frameworks (React, Vue, Next.js) save developers from writing everything from scratch.

Question Bank — Lesson 3-3

Part 1: Fill in the blanks

1. The technology that defines the structure of a web page is .....
2. The technology that specifies colors, layout and fonts is .....
3. The technology that adds behavior and interactivity is .....
4. Describing each part of a page with tags that indicate their meaning is called .....
5. The two benefits of semantic HTML are improved ..... and improved .....
6. A design in which the layout adjusts automatically to the screen size is .....
7. Prioritizing small screens from the design stage is called .....
8. A structure providing ready-made functions and components is a .....
9. The framework developed by Meta is ....., and the one that adds page-speed mechanisms to it is .....
10. The tag used at the top of a page is ..... and the one for navigation is .....

Part 2: Choose the correct answer

1. Which technology adds behavior to a web page?
   (a) HTML (b) CSS (c) JavaScript (d) JSON
2. CSS is compared in the textbook to:
   (a) the frame of a building (b) the interior and exterior of a building (c) the electrical system (d) the foundation

3. Semantic HTML improves accessibility because:

   (a) it makes pages load faster (b) screen readers can correctly understand the page structure
   (c) it reduces the number of images (d) it encrypts the page

4. Responsive design means:

   (a) a separate page for every device (b) the layout adjusts automatically to screen size (c) faster servers
   (d) using more JavaScript

5. The main benefit of using a framework is:

   (a) pages need no HTML (b) developers need not write all code from scratch (c) no server is required (d) CSS becomes unnecessary

6. Which framework is described as having a simple structure and allowing incremental building?

   (a) React (b) Vue (c) Next.js (d) JSON

7. Which of the following is a **semantic** tag?

   (a) a plain box with no meaning (b) <nav> (c) a coloured rectangle (d) a status code

8. Improved SEO means:

   (a) the site is encrypted (b) search engines understand the content and display it appropriately
   (c) the site loads without CSS (d) the site works offline

9. A library page lists books and filters results as the user types. The filtering is done by:

   (a) HTML (b) CSS (c) JavaScript (d) the database only

10. React is described as:

    (a) suited to large-scale applications, updating only part of the screen (b) a data format
    (c) a communication protocol (d) a type of database

Part 3: True (✓) or False (✗) — correct the false statements

1. HTML is a technology that defines the structure (skeleton) of a web page. ( )
2. CSS is a technology that adds behavior to a web page. ( )
3. Responsive design is a concept in which the layout is automatically adjusted according to screen size. ( )
4. Using a framework eliminates the need to write all code from scratch. ( )
5. Semantic HTML has no effect on how search engines read a page. ( )
6. HTML, CSS and JavaScript each have independent roles and are used in combination. ( )

Part 4: Match each role with the correct technology

Role	Options
1) Defines the structure of a web page	(a) HTML (b) CSS (c) JavaScript
2) Specifies the appearance of a web page	

3) Adds behavior and interactivity to a web page	

Part 5: Extended-response questions

1. **Explain why** a screen reader understands a page better when it uses <header>, <nav> and <main> instead of plain boxes.
2. **Explain why** responsive design is more practical than building a separate page for each device.
3. **Explain why** a team might choose a framework for a large project.
4. **Exam-style question [6 marks]:** Explain how HTML, CSS, and JavaScript each contribute to a library page that lists books, is styled, and filters the results as the user types. Refer to structure, appearance, and behavior.
5. **In a new context:** A school website looks correct on a laptop but is unreadable on phones, and blind students report that their screen reader jumps around. Identify the two techniques the site is missing and explain what each one would fix.

Chapter Test

Chapter 3 — Web Applications

Instructions

Time: 1 hour · Total marks: 40 · Answer all questions.

Question 1: Choose the correct answer [10 marks]

1. An application used through a browser with nothing to install is a:
   (a) desktop program (b) web application (c) database (d) protocol
2. The tier that processes data and makes decisions on the server is the:
   (a) frontend (b) backend (c) database (d) browser
3. Storing order history belongs to the:
   (a) frontend (b) backend (c) database (d) API
4. The side that requests data or processing is the:
   (a) server (b) client (c) database (d) framework
5. The method used to retrieve data from the server is:
   (a) POST (b) GET (c) JSON (d) API
6. Status code 500 means:
   (a) success (b) a problem on the server side (c) page not found (d) encrypted connection
7. A system for exchanging data between different pieces of software is an:
   (a) HTML (b) API (c) SEO (d) OS
8. The technology that specifies colors, layout and fonts is:
   (a) HTML (b) CSS (c) JavaScript (d) JSON
9. Layout adjusting automatically to screen size is called:
   (a) semantic HTML (b) responsive design (c) SEO (d) mobile framework
10. HTTPS differs from HTTP by adding:
    (a) more methods (b) TLS encryption (c) JSON support (d) a database

Question 2: Fill in the blanks [8 marks]

1. The screen component users see directly is the .....
2. The three tiers cooperating form the .....
3. The side that processes requests and returns responses is the .....

4. The HTTP method for sending data to the server is .....
5. Status code 404 means .....
6. The data format easy for humans and computers alike is .....
7. Using tags that indicate meaning is called .....
8. Ready-made functions and components for efficient development form a .....

Question 3: True (✓) or False (✗) — correct the false statements [6 marks]

1. The backend is the part that runs on the browser. ( )
2. A database organizes, stores, and manages data. ( )
3. The GET method is for sending data to the server. ( )
4. HTTPS adds encryption to HTTP. ( )
5. CSS adds behavior to a web page. ( )
6. Semantic HTML improves accessibility and SEO. ( )

Question 4: Match the two columns [4 marks]

(A)	(B)
1) Server-side processing users do not see	(a) database (b) backend (c) JavaScript (d) frontend
2) The screen users interact with directly	
3) Organizes, stores and manages data	
4) Adds behavior and interactivity to a page	

Question 5: Extended response [12 marks]

1. **[4 marks]** Explain how the three tiers cooperate when a user searches for a product on a shopping site.
2. **[4 marks]** Explain the difference between GET and POST, and between status codes 404 and 500.
3. **[4 marks]** Explain the roles of HTML, CSS and JavaScript, and say what semantic HTML adds.

Model Answers

Chapter 3 question banks and chapter test

Lesson 3-1 — Answers

Part 1: Fill in the blanks

1) Web application. **2)** Frontend. **3)** Backend. **4)** Database. **5)** Frontend — backend — database. **6)** Browser — server. **7)** Three-tier architecture. **8)** Backend — database.

Part 2: Multiple choice

1) c **2)** d **3)** b **4)** a **5)** b **6)** c **7)** a **8)** a **9)** b **10)** c

Note on (1): the **backend** issues the search, but the tier that actually searches through the stored data is the **database**.

Part 3: True / False

1) ✓ **2)** ✗ — the backend runs on the **server**, not on the browser. **3)** ✓ **4)** ✗ — it operates with **three tiers**: frontend, backend and database. **5)** ✗ — a web application needs **no dedicated software installed**; a browser is enough. **6)** ✓

Parts 4 and 5

Part 4: **1)** b **2)** a **3)** c

Part 5: **1)** a **2)** b **3)** c **4)** a **5)** b **6)** c

Part 6: Extended response

1) Because the frontend only **shows and collects**. It cannot process decisions or store data, so without a backend to process the request and a database to hold and retrieve the data, nothing could be searched, saved or returned.

2) Because every service does the same three kinds of work: showing a screen and taking input, processing and deciding, and storing and retrieving data. Only the **content of each job** differs — recommending videos, deciding a post's audience, or checking stock.

3) Answer points: the **frontend** shows the upload screen, lets the user choose the photo and add a caption, and sends them off. The **backend** receives the upload, checks the user is logged in and permitted, processes the image and decides who should see the post. The **database** stores the photo data, the caption, the timestamp and the link to the user's account, and later retrieves it when followers open their timeline. The result travels back up: database → backend → frontend → screen.

4) The **frontend** is clearly working, because the page opened and displayed correctly. The failure is most likely in the **backend or the database** — the request for free slots was not processed or the data was not returned; the missing part is data, not display.

5) Taking the city name → frontend. Looking up the forecast data → backend (requesting) and database (holding it). Storing past forecasts → database. A job the frontend cannot do on its own: retrieving or storing the forecast data — it has no access to stored data without the backend.

Lesson 3-2 — Answers

Part 1: Fill in the blanks

1) Client. **2)** Server. **3)** HTTP. **4)** HTTPS. **5)** GET — POST. **6)** Status code. **7)** 200 — 404 — 500. **8)** API. **9)** JSON. **10)** https://

Part 2: Multiple choice

1) c **2)** b **3)** b **4)** b **5)** b **6)** b **7)** b **8)** b **9)** b **10)** b

Part 3: True / False

1) ✓ **2)** ✓ **3)** ✗ — **GET retrieves** data from the server; **POST** sends data to it. **4)** ✓ **5)** ✓ **6)** ✗ — JSON is designed to be **easy for humans to read** as well as for computers to process.

Part 4: Matching

1) a **2)** b **3)** c

Part 5: Extended response

1) Because the password and other login details travel across the network. With plain HTTP the content is not encrypted, so a third party could read it; HTTPS adds **TLS encryption**, which reduces that risk.

2) **404** means the requested page does not exist — the address asked for is not there. **500** means a problem occurred **on the server side**, so the fault is not with what the user typed but with the server's own processing.

3) Because they declare different intentions: GET says "give me data" and is used for displaying pages and search results; POST says "here is data for you" and is used for login details and form contents. Using the wrong one misstates what the client wants and can expose submitted data.

4) Answer points: the **client** (browser) sends a **request** to the server, including an **HTTP method** — GET when it wants to retrieve a page. The server receives the request, processes it, finds the page, and returns a **response**. The response carries a **status code** reporting the result: 200 if it succeeded, 404 if the page does not exist, 500 if the server itself failed. The browser then renders the returned content, or shows an error message based on the code.

5) The **API** is the agreed system through which the weather app requests data from the other company's software and receives it back. The data is likely to arrive in **JSON** format. On a 500 code the app should tell the user that the **weather service is temporarily unavailable** — the fault is on the provider's server, not with the user's input — and offer to retry.

Lesson 3-3 — Answers

Part 1: Fill in the blanks

1) HTML. **2)** CSS. **3)** JavaScript. **4)** Semantic HTML. **5)** Accessibility — SEO. **6)** Responsive design. **7)** Mobile-first. **8)** Framework. **9)** React — Next.js. **10)** <header> — <nav>

Part 2: Multiple choice

1) c **2)** b **3)** b **4)** b **5)** b **6)** b **7)** b **8)** b **9)** c **10)** a

Part 3: True / False

1) ✓ **2)** ✗ — CSS specifies the **appearance**; adding behavior is **JavaScript**. **3)** ✓ **4)** ✓ **5)** ✗ — semantic HTML **improves SEO**, because search engines understand the content more easily. **6)** ✓

Part 4: Matching

1) a **2)** b **3)** c

Part 5: Extended response

1) Because those tags **carry meaning**: they tell the software which part is the page header, which is navigation and which is the main body. A screen reader can then announce the structure and let the user jump to the right section, instead of reading through undifferentiated boxes.

2) Because with responsive design a **single page** adapts its layout to any screen, so there is one set of content to write, update and fix, rather than separate versions that can drift out of step with each other.

3) Because a framework provides commonly used functions and components **in advance**, so the team does not write everything from scratch; development becomes faster and more consistent, and React in particular can update only part of the screen efficiently, which suits large applications.

4) Answer points: **HTML** provides the **structure** — the list of books, each entry's title and author, the search box. **CSS** provides the **appearance** — the layout of the list, colours, spacing and fonts. **JavaScript** provides the **behavior** — it reacts as the user types, filters the displayed books, and updates only that part of the screen without reloading the page. All three are needed together: structure alone would be unstyled and inert.

5) The site is missing **responsive design** and **semantic HTML**. Responsive design would make the layout adjust

automatically to phone screens so the content is readable. Semantic HTML would let the screen reader understand the page structure — header, navigation, main content — so it announces sections in a sensible order instead of jumping around.

Chapter 3 Test — Answers

Question 1

1) b **2)** b **3)** c **4)** b **5)** b **6)** b **7)** b **8)** b **9)** b **10)** b

Question 2

1) Frontend. **2)** Three-tier architecture. **3)** Server. **4)** POST. **5)** Page not found. **6)** JSON. **7)** Semantic HTML. **8)** Framework.

Question 3

1) ✗ — the backend runs on the **server**. **2)** ✓ **3)** ✗ — GET **retrieves**; POST sends. **4)** ✓ **5)** ✗ — CSS specifies **appearance**; JavaScript adds behavior. **6)** ✓

Question 4

1) b **2)** d **3)** a **4)** c

Question 5

1) The frontend receives the search keywords and sends them to the backend; the backend searches the database for matching products; the database returns the data; the backend organizes the results and returns them to the frontend; the frontend displays them on screen.

2) **GET** retrieves data from the server (displaying a page, search results); **POST** sends data to the server (login details, form contents). **404** means the requested page does not exist; **500** means the problem occurred on the server side.

3) HTML defines the structure, CSS specifies the appearance, JavaScript adds behavior and interactivity. **Semantic HTML** adds meaning to the structure by using tags such as <header>, <nav> and <main>, which improves accessibility for screen readers and improves SEO.

Appendix A — Mind Maps

One per lesson, for fast revision before the exam

1-1 Development of Information Technology and Social Transformation

Development of Information Technology

Stages of development

- 1940s–60s: ENIAC · military and scientific use
- 1970s–80s: personal computers (PCs)
- 1990s: commercial Internet and the Web
- 2000s: smartphones · mobile Internet
- 2010s onward: cloud computing · IT as a service

Moore's Law

- Empirical observation, not a physical law
- Transistors double about every 2 years
- Limits: leakage current · quantum tunneling
- Alternatives: multi-core · parallel processing

Social changes

- SNS — rapid information spreading
- E-commerce — Amazon, eBay
- Remote work
- Online learning
- Cashless payment — cards, QR, apps

Emerging technologies

- Autonomous driving + edge computing
- AR — overlays digital on the real world
- VR — full virtual immersion
- Quantum computing — qubit and superposition

1-2 How AI Works

How AI Works

Artificial Intelligence

- Broad field: learning · prediction · recognition · generation
- Most systems are narrow AI
- Examples: speech, image recognition, translation

Machine Learning

- A branch of AI
- Learns patterns from data, not explicit rules
- Examples: spam filtering · recommendation

Deep Learning

- A method within machine learning
- Multi-layer neural networks
- Weights change during training
- Needs relatively large data

Generative AI

- Creates new content
- Mostly built on deep learning
- Risk of hallucination: plausible but wrong
- Remedy: verify output and sources

1-3 AI in Daily Life and Industry

AI in Daily Life and Industry

Daily life

- Recommendation systems — predict preferences
- Voice assistants — recognise and execute commands
- Machine translation
- Face recognition

Industry

- Healthcare: image diagnosis · drug discovery
- Agriculture: harvest timing · pest detection
- Manufacturing: quality inspection · predictive maintenance
- Logistics: route optimisation

Good at

- Finding and classifying patterns
- Recognising images, sound and text
- Probabilistic inference and prediction

Requires caution

- Ethical judgments and bias
- Personal information and privacy
- High-impact decisions and responsibility
- Insufficient or biased training data
- Hallucination · copyright · black box

1-4 Ethical Issues with AI

Ethical Issues with AI

Algorithmic bias

- Unfair or harmful outcomes
- Sources: data · design · use · context
- Not caused by processing speed
- Examples: biased hiring · less accurate face recognition

Privacy

- Surveillance via face recognition
- Mass collection of behaviour data
- Control over shared personal data

XAI and responsibility

- XAI: understanding the factors behind an output
- Black box: unclear judgment process
- Responsibility: developer · operator · user
- Accountability: who is answerable, not who explains

The four principles

- Fairness — no unjust discrimination
- Transparency — clear process and limits
- Privacy protection
- Accountability — identifying responsible parties

2-1 Cryptographic Technologies and Authentication

Cryptography and Authentication

HTTPS and TLS

- HTTP carried over secured TLS
- Confidentiality + integrity + identity check
- Does not guarantee honest site content

TLS handshake

- 1) Digital certificate: verify identity and domain
- 2) Session keys derived, never sent
- 3) Data exchanged with common-key cryptography

Two cryptographies

- Public-key: shares keys safely
- Common-key: exchanges data quickly
- Division of roles = security + speed

Authentication

- MFA: two or more of three factors
- Knowledge · possession · biometric
- Banking: password + one-time password
- Common error: password + secret question

Combining technologies

- Encryption blocks reading
- Certificate proves the partner is authentic
- Signature detects tampering, gives non-repudiation
- MFA prevents unauthorized logins

2-2 Network Security Design

Network Security Design

Firewall

- Allows or denies by preset rules
- At boundary, between parts, or on a host
- e.g. allow web server, deny direct DB access

VPN

- Encrypted virtual private line (tunnel)
- Remote work · connecting branches
- Reduces eavesdropping on public Wi-Fi
- Does not delete viruses

DMZ

- Public-facing servers separated from internal network
- Limits damage if a public server is attacked
- Not about speed, not exposing all servers

Defense in depth

- Layer 1: network entry — firewall
- Layer 2: communication path — VPN
- Layer 3: server placement — DMZ
- Layer 4: endpoints — antivirus and OS updates

Zero trust

- Trust no communication, verify every access
- Even from inside the organization
- Caused by cloud services and remote work

2-3 Incident Response and Risk Management

Incident Response and Risk Management

Security incident

- Actual damage from an information security problem
- Information leak
- Data tampering
- Service outage

Six stages

- 1) Preparation: procedures set in advance
- 2) Detection: confirm an incident occurred
- 3) Containment: stop damage spreading
- 4) Eradication: remove the cause
- 5) Recovery: restore normal state
- 6) Prevention of recurrence

Why order matters

- Contain before eradicate
- Recovery without cause = incident repeats
- Backups make recovery possible

Risk assessment

- Risk size = impact × likelihood
- Impact: how much damage
- Likelihood: how probable
- High impact × high likelihood first

3-1 The Overall Structure of Web Applications

Structure of Web Applications

Web application

- Used through a web browser
- No dedicated software to install
- YouTube · Amazon · Gmail · Google Maps

Frontend

- The screen users see directly
- Runs on the browser, accepts input
- Search screen · product lists · forms

Backend

- Server-side processing users do not see
- Processes data and makes decisions
- Product search · login authentication

Database

- Organizes, stores and manages data
- Retrieves when needed, records new data
- Products · users · order history

How they cooperate

- Frontend shows and collects
- Backend decides and processes
- Database stores and retrieves
- Request flows down, reply returns up

3-2 Web Application Communication Methods

Web Communication Methods

Client and server

- Client requests: browser, phone app
- Server processes and responds
- Request → response cycle

Protocols

- HTTP: exchanges data client↔server
- HTTPS: HTTP + TLS encryption
- URLs starting https:// are encrypted

Methods and codes

- GET retrieves data from the server
- POST sends data to the server
- 200 success · 404 not found · 500 server error

API and JSON

- API exchanges data between software
- Frontend calls backend through an API
- JSON: readable by humans and computers

3-3 Fundamentals of Frontend Technology

Frontend Technology

The three technologies

- HTML: structure — the building frame
- CSS: appearance — the interior
- JavaScript: behavior — the wiring
- Independent roles, used in combination

Semantic HTML

- Tags that indicate meaning
- header · nav · main · footer
- Improves accessibility for screen readers
- Improves SEO

Responsive design

- Layout adjusts to screen size
- One page works on every device
- Mobile-first: small screens come first

Frameworks

- Ready-made functions and components
- React: partial updates, large apps
- Vue: simple, incremental
- Next.js: React plus faster page display

Appendix B — Extra Question Bank

Short questions with answers for every lesson

Lesson 1-1 — Development of Information Technology and Social Transformation

Q1: What is the difference between edge computing and cloud computing in terms of where processing happens?
A: Edge computing processes data on the device itself, instantly; cloud computing delivers IT resources as a service over the Internet and processing happens on remote servers.

Q2: Why are devices described as having become 'smaller and more connected'?
A: Because development moved from computers filling a whole room to personal computers and then smartphones, and with the spread of the Internet these devices became connected to each other and to services.

Q3: In which stage did email emerge as a prominent social impact?
A: In the 1990s, with the commercialization of the Internet and the appearance of the Web.

Q4: Name two approaches used to improve performance other than shrinking transistors.
A: Parallel processing using multiple processor cores, and quantum computers based on quantum mechanics.

Q5: What role do cameras and sensors play in an autonomous vehicle?
A: They recognise the vehicle's surroundings; the system then processes this data to make driving decisions and control the vehicle.

Q6: Explain why quantum computing is not a general replacement for classical computers.
A: Because it is expected to help with specific classes of difficult computations, and does not speed up every kind of calculation.

Q7: What is the difference between a bit and a qubit?
A: A classical bit holds one state, whereas a qubit uses the principle of superposition.

Q8: Classify: 'a student attending a lesson online' — which social change?
A: Online learning.

Q9: Why might a fully cashless society be a concern?
A: Because it may exclude people who have no bank card or smartphone, and it makes everyone dependent on network and system availability.

Q10: What do personal computers and smartphones have in common in terms of social impact?
A: Both moved technology to the level of the individual: PCs began personal computer use, and smartphones spread the Internet widely through mobile devices.

Q11: Name two e-commerce platforms mentioned in the lesson.
A: Amazon and eBay.

Q12: What is the connection between the spread of cloud computing and large-scale data analysis?
A: The cloud provided storage and processing resources delivered as a service over the Internet, which made large-scale data analysis and widespread AI use possible.

Lesson 1-2 — How AI Works

Q1: What is the essential difference between a rule-based system and a machine-learning system?
A: The first follows rules written explicitly by a programmer; the second learns patterns from data without every rule being programmed.

Q2: What does it mean that most AI systems are 'narrow'?
A: They are designed for a specific task or a limited set of tasks, and are not a general intelligence that can do everything.

Q3: What is an artificial neural network made of?
A: Connected units whose weights change during training so the network can learn patterns from data; it is loosely inspired by connected neurons.

Q4: Why is the relationship between the four concepts described as 'simplified'?
A: Because it is a teaching illustration and should not be read as strict containment in every case.

Q5: Give two examples of tasks deep learning is good at.
A: Image analysis and speech recognition.

Q6: What kinds of content can generative AI produce?
A: Text, images, audio and software.

Q7: A student used a generative tool and received a scientific reference that does not exist. What is this called, and what is the correct action?
A: Hallucination; the correct action is to verify the output and its sources before using it.

Q8: Explain why not every AI system can be called a machine-learning system.
A: Because AI is a broader field containing several approaches, and machine learning is one of its branches, not all of it.

Q9: What allows deep learning to learn complex patterns?
A: Its use of multi-layer neural networks that learn layered representations from data.

Q10: Classify: 'automatic speech recognition in a voice assistant'.
A: Deep learning (which is at the same time within machine learning and within AI).

Q11: Why does deep learning need relatively large amounts of data?
A: So that it can learn reliable patterns; too few examples leave the model unable to generalise accurately.

Q12: State three tasks AI performs according to the lesson definition.
A: Learning from data, prediction, and recognition (as well as content generation and making or supporting decisions).

Lesson 1-3 — AI in Daily Life and Industry

Q1: What data does a recommendation system rely on?
A: The user's past behaviour data, from which it predicts preferences and displays recommendations.

Q2: Name two AI tasks in the healthcare sector.
A: Image diagnosis to detect disease, and supporting drug discovery.

Q3: What is the difference between predictive maintenance and quality inspection in manufacturing?
A: Predictive maintenance forecasts machine failures before they occur; quality inspection checks the product itself during or after production.

Q4: Explain why a correct AI result is not by itself enough for a high-impact decision.
A: Because a high-impact decision also requires clarity about how the result was reached and a clear allocation of responsibility, which the system alone does not provide.

Q5: When do AI judgments become inaccurate?
A: When the training data is insufficient, unrepresentative or biased.

Q6: What is meant by the black box problem?
A: That it is unclear how the system reached its judgment, making it hard to evaluate and hard to detect its errors.

Q7: Name a rights issue connected to AI training data.
A: The use of copyrighted works as training data.

Q8: Why do AI services raise privacy concerns?
A: Because they often use personal data about the user's behaviour: what they watch, buy and say.

Q9: Classify: 'optimising delivery truck routes'.
A: Logistics.

Q10: A factory wants to reduce sudden production-line stoppages. Which technology fits, and why?
A: Predictive maintenance, because it uses data to forecast equipment failures before they occur, allowing action in advance.

Q11: Name three areas AI is good at.
A: Finding and classifying patterns, recognising images, sound and text, and probabilistic inference and prediction.

Q12: Why does the need for human oversight grow as the impact of a decision rises?
A: Because the cost of an error to people and their rights becomes large, and the system guarantees neither the correctness nor the fairness of the result, nor does it bear responsibility for it.

Lesson 1-4 — Ethical Issues with AI

Q1: What is meant by a 'proxy variable' in the context of bias?
A: A variable that indirectly represents a protected attribute, so using it can produce discrimination even without naming the attribute explicitly.

Q2: Name two sources of algorithmic bias other than the data.
A: How the system is built (choice of variables and model design), and how it is used together with the human and social context.

Q3: What exactly does XAI do?
A: It helps people understand the factors that contributed to the system reaching a particular output or decision.

Q4: Why is bias hard to detect in a non-transparent system?
A: Because lack of clarity about how the result was reached prevents it from being evaluated and prevents errors or bias from being found.

Q5: Between which parties may responsibility be distributed?
A: The developer, the operating organisation, and the user.

Q6: Is there a single allocation of responsibility that fits every context? Why?
A: No, because it varies with the system, the use and the applicable rules.

Q7: Name the two prominent privacy issues linked to the spread of AI.
A: Surveillance through face-recognition technology, and the mass collection and analysis of personal data.

Q8: 'Disclosing the decision-making process to users in an understandable way' — which principle?
A: Transparency.

Q9: 'Not using collected data for anything other than its original purpose' — which principle?
A: Privacy protection.

Q10: Explain why slow processing is not a cause of algorithmic bias.
A: Because bias arises from the data, the system design, the way it is used or its context — not from hardware performance.

Q11: How can bias be reduced in practice before a hiring system goes live?
A: By checking how well the training data represents different groups, testing outcomes across those groups, and reviewing the model design and the context of use.

Q12: What is the relationship between the black box problem and the principle of transparency?
A: The black box problem is exactly what transparency and XAI methods address, by providing clear information about the system, its decision process and its limits.

Lesson 2-1 — Cryptographic Technologies and Authentication

Q1: What does the browser check in a digital certificate?
A: Its validity, its chain of trust, and that it matches the name of the site being visited.

Q2: Why is the session key itself never sent across the network?
A: Because it is derived at each side from shared secrets the two parties negotiate, so an eavesdropper cannot capture it.

Q3: What is the purpose of integrity mechanisms during data exchange?
A: To detect any alteration made to the data while it is in transit.

Q4: Give one example for each of the three authentication factors.
A: Knowledge: a password. Possession: a smart card or a one-time code on a phone. Biometric: a fingerprint or face.

Q5: Why is a possession factor a good complement to a password?
A: Because it is independent of it: someone who knows the password does not necessarily hold the device or card required.

Q6: What does non-repudiation mean?
A: That the system provides evidence preventing the signer from denying that they signed or sent the message.

Q7: Explain why HTTPS does not protect you from a fraudulent site that holds a valid certificate.
A: Because the certificate only proves the server's identity and its link to the domain; it makes no judgement about the honesty of the content or the owner's intentions.

Q8: Put in order: (data exchange — deriving session keys — checking the certificate).
A: Checking the certificate → deriving session keys → data exchange.

Q9: Name the four threats addressed by combining security technologies.
A: Eavesdropping, tampering, impersonation, and unauthorized login.

Q10: Why is common-key cryptography described as better suited to session data?
A: Because it exchanges large amounts of data quickly, while using public-key cryptography for everything would be too slow.

Q11: What authentication combination does a company laptop login use in the textbook example?
A: A smart card (possession) plus fingerprint authentication (biometric).

Q12: A school wants a fee portal, but a student has no smartphone. How do you balance security with accessibility?
A: By offering an alternative second factor that does not depend on a smartphone (a printed code or a hardware security key), so that requiring security does not exclude a group of students.

Lesson 2-2 — Network Security Design

Q1: Where can a firewall be located?
A: At the network boundary, between parts of a network, or on a host machine.

Q2: Give a typical firewall rule example.
A: Allow access to the web server, but deny direct external access to the database server.

Q3: What two techniques does a VPN rely on?
A: Encryption and tunnelling.

Q4: Which servers are placed in a DMZ?
A: Servers exposed to the external network, such as web servers and mail servers.

Q5: Explain why the customer database is placed in the internal network and not in the DMZ.
A: Because it holds confidential data that should not be exposed to the Internet, unlike servers the public needs to reach.

Q6: Which layer addresses the threat of eavesdropping on a public network?
A: The communication-path layer, using a VPN.

Q7: Which layer addresses an employee's device being infected with malware?
A: The endpoint layer: antivirus software and keeping the OS updated.

Q8: Summarise the premise of traditional security in one sentence.
A: 'Inside the organization's network is safe, and outside is dangerous.'

Q9: What is checked on every access request under zero trust?
A: Identity verification and access-permission checks, performed every time.

Q10: Explain why separation alone is not enough to protect a public server.
A: Because the server is still exposed to attack; separation only limits the damage of a breach, so it needs other controls such as updates and access monitoring.

Q11: What is the difference between defense in depth and zero trust?
A: Defense in depth is about stacking layers of protection; zero trust is about granting no automatic trust and verifying every access.

Q12: A hospital moves records to the cloud and allows access from home. Name two measures and one remaining risk.
A: Measures: a VPN to protect the communication path, and verifying every access by identity and permissions. Remaining risk: compromise of the doctor's own device, or a leak from inside the organization.

Lesson 2-3 — Incident Response and Risk Management

Q1: What defines a security incident?
A: A situation in which actual damage occurs because of an information security problem.

Q2: What is the difference between containment and eradication?
A: Containment limits the scope of impact so damage does not spread; eradication removes the cause, such as the malware and the weakness that was exploited.

Q3: What does the recovery stage involve?
A: Returning systems and services to their normal state, often by restoring from a clean backup.

Q4: What is the purpose of the prevention-of-recurrence stage?
A: Analyzing the cause and taking measures so that the same incident does not happen again.

Q5: Why is the preparation stage carried out before any incident?
A: Because having procedures and structures ready in advance makes the response faster and better organised under pressure.

Q6: What can go wrong if recovery is performed without identifying the cause?
A: The same incident may occur again, because the malware or the exploited weakness is still present.

Q7: Two risks: large impact × low likelihood, and small impact × high likelihood. Which comes first?
A: The verbal description alone is not enough to rank them; the decision depends on the matrix scores, the context and the controls available.

Q8: Why does an organization not address every risk at once?
A: Because resources are limited, so priorities must be set using impact × likelihood.

Q9: Classify: 'grades altered in the school system without authorization'.
A: Data tampering.

Q10: Classify: 'the school website goes down because of an attack on the server'.
A: Service outage.

Q11: Which preventive control makes the recovery stage possible at all?
A: Having regular, clean backups — which is part of the preparation stage.

Q12: Name the three typical types of security incident.
A: Information leak, data tampering, and service outage.

Lesson 3-1 — The Overall Structure of Web Applications

Q1: What makes an application a 'web application'?
A: It is used through a web browser and needs no dedicated software installed.

Q2: Which tier accepts the user's input?
A: The frontend — it runs on the browser and receives what the user types or clicks.

Q3: Which tier decides whether a login is valid?
A: The backend, because authentication is server-side processing and decision making.

Q4: Where is order history kept on an e-commerce site?
A: In the database, which stores and manages the data.

Q5: List the six steps of a product search in order.
A: Frontend receives keywords → sends them to the backend → backend searches the database → database returns matching data → backend organizes results → frontend displays them.

Q6: What changes between a video site and an SNS in terms of tiers?
A: Nothing structurally — both use the same three tiers; only the specific job of each tier differs.

Q7: Name one backend job on a video sharing site.
A: Selecting recommended videos, or aggregating view counts.

Q8: Name one database job on an SNS.
A: Storing post data, follow relationships or messages.

Q9: A page loads but shows no data. What does that tell you?
A: The frontend is working (it rendered), so the failure is most likely in the backend or the database.

Q10: Why is the three-tier split better than one single program?
A: Each tier has a clear responsibility, so the system is easier to build, test, fix and scale, and a fault can be traced to one tier.

Q11: Which tier would handle checking which appointment slots are free?
A: The backend requests it and the database holds the slot data; the frontend only displays the result.

Q12: Give an example of a web application you use, and name its three tiers' jobs.
A: For example Gmail: frontend shows the inbox and compose screen, backend sorts and sends mail, database stores messages and contacts.

Lesson 3-2 — Web Application Communication Methods

Q1: What is a request and what is a response?
A: A request is what the client sends asking for data or processing; a response is what the server returns after processing it.

Q2: Give two examples of a client.
A: A web browser and a smartphone app.

Q3: Why do URLs beginning with https:// matter?
A: They indicate the connection uses HTTPS, so the content is encrypted and harder for third parties to read.

Q4: Which method would a search results page use, and why?
A: GET, because it retrieves data from the server rather than sending new data.

Q5: Which method sends form contents, and why?
A: POST, because form contents are data being sent to the server.

Q6: What does status code 200 mean?
A: Success — the request was processed successfully.

Q7: A user mistypes a web address. Which status code is likely?
A: 404 — the specified URL does not exist.

Q8: The server itself has crashed. Which status code is likely?
A: 500 — a problem occurred on the server side.

Q9: What does an API do in a web application?
A: It lets the frontend send requests to the backend and receive data, acting as an agreed system for exchanging data between software.

Q10: Why is JSON widely used for API data?
A: Because it is easy for humans to read and easy for computers to process.

Q11: Is JSON a programming language?
A: No — it is a data format used to describe exchanged data.

Q12: Two apps from different companies need to share data. What do they need?
A: An API — a defined system for exchanging data between different pieces of software.

Lesson 3-3 — Fundamentals of Frontend Technology

Q1: What does HTML define, and what is its analogy?
A: The structure or skeleton of the page — like the frame of a building.

Q2: What does CSS specify?
A: The appearance: colors, layout, size and fonts.

Q3: What does JavaScript add?
A: Behavior and interactivity — responses to button presses and updating only part of the screen.

Q4: Name four semantic tags and where they go.
A:
at the top,
for navigation,
for the body,
at the bottom.

Q5: How does semantic HTML help a visually impaired user?
A: Screen reader software can correctly understand the page structure, so information is easier to convey.

Q6: How does semantic HTML help search engines?
A: They understand the content more easily, making the page more likely to be displayed appropriately in results.

Q7: Define responsive design in one sentence.
A: A design concept in which the layout is automatically adjusted according to different screen sizes.

Q8: What is mobile-first?
A: Prioritizing small screens such as smartphones from the design stage.

Q9: What problem do frameworks solve?
A: Developers do not need to write all code from scratch, so development is more efficient.

Q10: Which framework suits a large application needing partial screen updates?
A: React, developed by Meta.

Q11: What does Next.js add beyond React?
A: Mechanisms to speed up page display.

Q12: A button on a page does nothing when clicked. Which technology is most likely at fault?
A: JavaScript, because behavior and interactivity are its role.

Appendix C — Teacher's Guide

Lesson planning, common mistakes, activities and assessment

1-1 Development of Information Technology and Social Transformation

Suggested teaching time

Two periods (90 minutes)

Lesson hook

Ask students: "How many digital services have you used since this morning?" Then ask which of them existed 30 years ago. This opens the lesson without any pre-teaching.

Common student misconceptions

- Students think Moore's Law is a fixed physical law — clarify that it is an observation about a historical trend.
- Confusing AR and VR — use the rule: "augmented adds to reality, virtual replaces reality".
- Believing quantum computing will replace all computers — correct this: specific classes of problems only.
- Confusing edge and cloud computing — always tie edge computing to the autonomous-driving example and response time.

Suggested classroom activity

Survey task: each student asks 10 classmates about their usual payment method (cash / card / app / QR), then fills a stakeholder table (customer, small shop owner, someone with no bank card) with one benefit and one drawback for each, ending with a recommendation supported by two reasons.

Assessment criteria — the student can:

- States the five stages in the correct chronological order.
- Defines Moore's Law and explains that it is not a physical law.
- Distinguishes the four emerging technologies with examples.

- Justifies edge computing using response time and safety.

Homework

Parts 1 and 2 of the question bank plus extended-response question 4.

1-2 How AI Works

Suggested teaching time

Two periods (90 minutes)

Lesson hook

Show three tasks: classifying a spam email, generating an image from text, recognising a face. Ask: is the computer following fixed rules here, or learning from examples?

Common student misconceptions

- The most common error: treating AI and ML as synonyms — draw the nested circles on the board before any verbal explanation.
- Treating deep learning as separate from machine learning — stress that it is a method within it.
- Assuming generative output is correct because it is written in fluent language — this is where hallucination is taught.
- Reading the hierarchy as strict containment — the textbook itself warns it is a simplified teaching relationship.

Suggested classroom activity

Nested-circles task: each student draws four nested circles and writes one example from their own life in each, then swaps papers with a partner and marks each other's work.

Assessment criteria — the student can:

- Orders the four concepts from broadest to most specific.
- Gives a correct example for each concept.
- Defines hallucination and proposes a suitable verification step.
- Explains why models fail on rare cases.

Homework

The whole question bank except the extended-response section, plus the 'In a new context' question.

1-3 AI in Daily Life and Industry

Suggested teaching time

One and a half periods (70 minutes)

Lesson hook

Ask students to name three services they used this week that they believe rely on AI, then ask: what data did each of them need?

Common student misconceptions

- Thinking machine translation means human translation aided by a computer — correct: fully automatic.
- Confusing predictive maintenance with routine maintenance — predictive uses data to forecast failure before it happens.
- Believing AI is good at ethical judgments — this is precisely the caution area.
- Mixing the 'good at' and 'requires caution' lists — train them on the rule: patterns, recognition and prediction it is good at; values, privacy and the final decision need humans.

Suggested classroom activity

Two-column sort: write 8 mixed scenarios on the board and have students sort them into 'good at' and 'requires caution' with one reason each.

Assessment criteria — the student can:

- Links four everyday services to their technologies.
- Links four industries to example uses.
- Distinguishes what AI is good at from what requires caution.
- Justifies human oversight using the impact-of-error criterion.

Homework

Multiple choice and true/false sections plus the exam-style question.

1-4 Ethical Issues with AI

Suggested teaching time

Two periods (90 minutes) — discussion-based lesson

Lesson hook

Present the situation: a face-recognition system that is less accurate for some groups. Before explaining anything, ask: who is harmed, and how?

Common student misconceptions

- The most common confusion: accountability versus XAI — drill it in: XAI answers 'why', accountability answers 'who is answerable'.
- Attributing bias to weak hardware or slow processing — correct: its source is the data, the design or the use.
- Assuming responsibility is predetermined in every case — clarify that it varies by system and context.
- Mixing transparency with privacy protection — transparency is about the system, privacy is about people's data.

Suggested classroom activity

Classroom tribunal: three groups represent the developer, the operating company and the user in an unfair hiring-decision case. Each group defends the limits of its own responsibility, then the class votes on how responsibility should be allocated, justifying the decision using the four principles.

Assessment criteria — the student can:

- Defines algorithmic bias and states two causes.
- Accurately links four situations to the four principles.
- Distinguishes accountability from XAI.
- Proposes a responsible-use rule justified by a named principle.

Homework

The complete question bank — this lesson generates the most exam questions.

2-1 Cryptographic Technologies and Authentication

Suggested teaching time

Two periods (90 minutes)

Lesson hook

Open a site that uses HTTPS, click the padlock in the address bar and show the certificate to the class. Ask: who issued this certificate, and why does the browser trust it?

Common student misconceptions

- Assuming HTTPS means the site itself is honest — correct it: it secures the connection only.
- Assuming all data is encrypted with public-key cryptography — clarify the division of roles: public-key shares keys, common-key carries data.
- The most dangerous error: treating 'password + secret question' as multi-factor — both are knowledge.
- Confusing the digital certificate with the digital signature — the certificate proves the server's identity, the signature proves a specific message's integrity.

Suggested classroom activity

Factor sorting game: write 12 verification methods on cards (password, fingerprint, smart card, one-time code, secret question, face…) and have students sort them into three baskets — knowledge / possession / biometric — then form valid MFA pairs and invalid ones.

Assessment criteria — the student can:

- Orders the three stages of the TLS handshake.
- Justifies the two cryptographies using security and speed.
- Distinguishes valid from invalid multi-factor authentication.
- Matches four threats to the technology that addresses each.

Homework

Parts 1, 2 and 4 of the question bank plus the exam-style question.

2-2 Network Security Design

Suggested teaching time

Two periods (90 minutes)

Lesson hook

Draw a school network on the board: public website, computer lab, student records. Ask: where would you place each part, and why?

Common student misconceptions

- Thinking a DMZ speeds up the connection or exposes all servers — its purpose is separation.
- Thinking a VPN removes viruses — a VPN protects the communication path only.
- Treating a firewall as complete protection — this is where the single-point-of-failure idea is taught.
- Reading zero trust as 'block access' — it means verify every access, not deny it.

Suggested classroom activity

Network design task: each group designs a network for a small company (public site + remote employees + confidential database), assigns each asset its threat and its protection layer, then presents while the class asks one question: 'what if this layer fails?'

Assessment criteria — the student can:

- Defines the four roles: firewall, VPN, DMZ, endpoint controls.
- Classifies measures into the four defense layers.
- Explains why one measure is not enough.
- Explains zero trust and why it emerged.

Homework

The whole question bank plus a network diagram drawn in the notebook.

2-3 Incident Response and Risk Management

Suggested teaching time

One and a half periods (70 minutes)

Lesson hook

Present a live scenario: 'The student records are encrypted and staff cannot log in — what do you do now?' Collect student suggestions before showing the six stages, then map their suggestions onto them.

Common student misconceptions

- Starting with recovery before eradication — use the ransomware example to show the malware would re-encrypt everything.
- Treating the order as unbreakable in every real case — explain that the sequence guides the work while investigation may reveal new information.
- Estimating risk from impact alone — drill the formula: impact × likelihood.
- Treating any outage as a security incident — a planned update is not.

Suggested classroom activity

Risk matrix task: each group identifies four risks facing the school, scores impact and likelihood from 1 to 3, places them on a matrix, ranks the priorities and justifies the first two actions.

Assessment criteria — the student can:

- States the six stages in order.
- Justifies containment coming before eradication.
- Applies the risk formula to given cases.
- Distinguishes a security incident from normal operation.

Homework

The whole question bank plus the 'In a new context' question written out.

3-1 The Overall Structure of Web Applications

Suggested teaching time

Two periods (90 minutes)

Lesson hook

Ask the class to open a shopping site and search for anything. Then ask: which part of what just happened did your phone do, and which part happened somewhere else?

Common student misconceptions

- Believing the backend runs in the browser — stress that it runs on the server.
- Thinking the frontend can work alone — it only shows and collects.
- Confusing backend with database: the backend decides, the database stores.
- Assuming a web application must be installed — a browser is enough.

Suggested classroom activity

Tier relay: give each group of three a service (video site, SNS, food delivery). Each student takes one tier and writes what their tier does for one user action, then the group performs the request as a relay in front of the class.

Assessment criteria — the student can:

- Defines the three tiers and their roles.
- Traces the six-step search flow in order.
- Classifies e-commerce items by tier.
- Diagnoses which tier failed from a described symptom.

Homework

Parts 1, 2 and 5 of the question bank plus the exam-style question.

3-2 Web Application Communication Methods

Suggested teaching time

Two periods (90 minutes)

Lesson hook

Open the browser developer tools network tab on any page and show the requests, their methods and their status codes. Ask: what did the browser ask for, and what did the server reply?

Common student misconceptions

- Swapping GET and POST — GET retrieves, POST sends; drill it with examples.
- Reading 500 as the user's mistake — it is a server-side fault.
- Thinking HTTPS is just 'a faster HTTP' — it adds TLS encryption.
- Treating JSON as a programming language — it is a data format.

Suggested classroom activity

Status code triage: give students six short scenarios (a mistyped URL, a crashed server, a successful search…) and have them assign 200, 404 or 500 to each and say whose side the problem is on.

Assessment criteria — the student can:

- Distinguishes client from server.
- Explains the difference between HTTP and HTTPS.
- Matches GET/POST and status codes to situations.
- Explains the role of an API and the JSON format.

Homework

The whole question bank plus the 'In a new context' question.

3-3 Fundamentals of Frontend Technology

Suggested teaching time

Two periods (90 minutes)

Lesson hook

Show a page, then disable its CSS in front of the class. Ask what disappeared and what stayed — that separation is the whole lesson.

Common student misconceptions

- Saying CSS adds behavior — CSS is appearance, JavaScript is behavior.
- Thinking semantic HTML changes how a page looks — it changes what it means.
- Confusing responsive design with building a separate mobile site.
- Thinking a framework replaces HTML and CSS.

Suggested classroom activity

Three-colour markup: print a screenshot of a familiar page and have students colour the parts by technology — structure, appearance, behavior — then defend one disputed area to the class.

Assessment criteria — the student can:

- Assigns structure, appearance and behavior to the right technology.
- Explains the two benefits of semantic HTML.
- Explains responsive design and mobile-first.
- Explains why frameworks improve efficiency.

Homework

The whole question bank plus the library-page exam-style question.

Appendix D — Parent's Guide

How to help your child study — no technical background needed

Before you start

This guide is written for a parent, not the student, and assumes no prior technical knowledge. For each lesson you get: a plain-language explanation, an everyday analogy, three questions to ask your child with the expected answer, warning signs that they have not understood, a short activity, and a suggested study time.

1-1 Development of Information Technology and Social Transformation

The lesson in plain language

This lesson tells the story of how technology developed in stages: first a computer that filled a whole room and was used by the military, then computers in homes, then the Internet, then smartphones, and finally 'the cloud' — meaning your programs and files run on distant machines rather than your own device. Each stage changed how people work, shop and learn.

An analogy that makes it click

Think of transport: first one expensive car that few people had, then a car in every home, then roads linking cities (the Internet), then hailing a ride from your phone (apps). Each stage added something and changed daily life.

Ask them these questions

1) Put these in the order they appeared: smartphone — computer — cloud computing — commercial Internet.
Expected answer: Computer → commercial Internet → smartphone → cloud computing. If the order is wrong, send them back to the stages table at the start of the lesson.

2) What is the difference between augmented reality and virtual reality?
Expected answer: Augmented adds digital things on top of the real world while you still see your surroundings; virtual places you inside a fully computer-made world. Mixing these up is the most common exam mistake here.

3) Why does a self-driving car process its data in the car itself rather than over the Internet?
Expected answer: Because even a small delay could cause an accident, so processing locally reduces response time. The term needed is 'edge computing'.

Signs they have not understood

- They say Moore's Law is a 'law of physics' — it is only an observation about a trend.
- They say quantum computing will replace all computers — no, it helps with certain problems only.

A 10-minute activity together

Sit with them for 10 minutes and ask: count the digital services you have used since this morning, and say which of the five social changes each one belongs to (social networking / e-commerce / remote work / online learning / cashless payment).

Suggested study time

45 minutes to study + 20 minutes on questions

1-2 How AI Works

The lesson in plain language

This lesson makes clear that 'artificial intelligence' is a broad name with narrower kinds inside it. The key idea your child must grasp: computers used to follow rules a programmer wrote by hand; now they learn on their own from a large number of examples. The newest kind writes new text and images — and that is the kind that can produce convincing but wrong answers.

An analogy that makes it click

Like teaching a child to tell a cat from a dog. You can give a rule — 'whiskers means cat' — that is old-style programming. Or show them a thousand pictures until they work it out themselves — that is machine learning. And if all thousand pictures were white cats, they will get it wrong the first time they see a black one.

Ask them these questions

1) Order these from broadest to narrowest: deep learning — artificial intelligence — generative AI — machine learning.
Expected answer: AI → machine learning → deep learning → generative AI. This appears in nearly every exam.

2) What does 'hallucination' mean here?
Expected answer: The system produces something that looks correct and convincing but is not true. The fix is to check the fact and its source before using it.

3) Why does AI get rare things wrong?
Expected answer: Because it learns from many examples; if something is rare in the training data there are not enough patterns for it to recognise it.

Signs they have not understood

- They say 'AI' and 'machine learning' mean the same thing — no, the second sits inside the first.
- They believe whatever an AI app tells them — that is exactly what this lesson warns against.

A 10-minute activity together

Draw four circles inside each other together on paper, and write in each one the name of the concept plus one example from your own life. That single drawing fixes the lesson in memory.

Suggested study time

45 minutes to study + 20 minutes on questions

1-3 AI in Daily Life and Industry

The lesson in plain language

This lesson says AI is very good at some things and unsuited to others. Good at: finding patterns, recognising images and sound, and predicting. Not to be left alone with: ethical judgments, personal data, and the final decision that somebody has to answer for.

An analogy that makes it click

Like an assistant who is excellent at sorting and calculating, but whom you would not let decide who gets hired and who does not. Mechanical work: yes. Decisions involving conscience and responsibility: no.

Ask them these questions

1) Name two things AI is good at and two things that need caution.
Expected answer: Good at: patterns, recognising images and sound, prediction. Caution: ethics, privacy, the final decision and responsibility.

2) Why must a human doctor review an AI reading of an X-ray?
Expected answer: Because the cost of an error is high for the patient, the system can be wrong if its data is incomplete or biased, and responsibility must rest with a person.

3) What links a spam filter and a shopping recommendation system?
Expected answer: Both learn patterns from data and predict; neither runs on rules a programmer wrote by hand.

Signs they have not understood

- They memorise the two lists wrongly and put 'ethical judgments' under what AI is good at — a frequent mistake.
- They see no problem with apps collecting their personal data.

A 10-minute activity together

Ask them about 5 services you use at home (video, maps, banking) and have them tell you: what is the AI doing in each, and what data is it taking from you?

Suggested study time

35 minutes to study + 20 minutes on questions

1-4 Ethical Issues with AI

The lesson in plain language

This lesson is about the unfairness AI can cause. The core idea: if the data it learned from contains discrimination, it will repeat that discrimination. The lesson then sets out four principles: fairness, openness about how decisions are made, protecting personal data, and naming who is responsible.

An analogy that makes it click

If a manager hired only men for twenty years, and you then bring in a computer that learns from those old hiring files, the computer will learn the same bias. Not because it is malicious, but because that is all it saw.

Ask them these questions

1) If a hiring system unfairly rejects a group, what is the likely cause?
Expected answer: Biased training data, or the design of the system itself. Not the computer's speed — that wrong answer is deliberately put among the choices.

2) What is the difference between transparency and accountability?
Expected answer: Transparency explains how the decision was made. Accountability names who answers for the result. Confusing the two is the biggest error in this lesson.

3) A school wants face-recognition cameras at the gate. What is the benefit and what is the concern?
Expected answer: Benefit: fast, accurate attendance. Concern: collecting students' biometric data and the possibility of tracking them. Responsibility is shared between the school and the manufacturer.

Signs they have not understood

- They blame bias on a slow device or weak Internet — completely wrong.
- They say accountability means 'explaining the decision' — no, that is XAI.

A 10-minute activity together

Discuss a real situation: if an app refused you a loan or a service without telling you why, how would you feel, and what would you have wanted to know? That conversation teaches transparency better than memorising ever will.

Suggested study time

50 minutes to study + 25 minutes on questions — this lesson generates the most exam questions

2-1 Cryptographic Technologies and Authentication

The lesson in plain language

This lesson explains what happens when you open a bank site or buy something online. Three things happen: the conversation is scrambled so nobody can read it, the browser checks the site is genuine and not a fake, and to enter your account it asks for two things rather than one.

An analogy that makes it click

Like sending an important letter: you seal it in an envelope (encryption), you check the address really belongs to the right person (the digital certificate), and you sign it so nobody can claim you did not send it (the digital signature). Two-factor login is like the bank asking for both the card and the PIN — the card alone is not enough.

Ask them these questions

1) Why is 'password + secret question' not counted as two-factor?
Expected answer: Because both are the same kind of thing: something you know. The two factors must be of different kinds — something you know plus something you have or something you are.

2) If someone steals your password, why is the account still protected?
Expected answer: Because a second, independent factor is needed — a code sent to your phone — and the thief does not have your phone.

3) If a site shows https, does that mean the site is honest?
Expected answer: No. It secures the connection only and says nothing about the content. This question is set deliberately to catch students out.

Signs they have not understood

- They think all the data is encrypted the same way — there are two kinds, each with its own job.
- They call any two-step check 'two-factor' without looking at what kind each factor is.

A 10-minute activity together

Open any site with a padlock next to the address, click it and view the certificate. Ask them: who issued this certificate, and why does the browser trust it?

Suggested study time

45 minutes to study + 25 minutes on questions

2-2 Network Security Design

The lesson in plain language

This lesson says network protection is not one lock but layers. A firewall decides who may come in and go out, a VPN creates a private encrypted line when you work from home, and a DMZ puts the servers the public can reach in a separate place away from the company's confidential data.

An analogy that makes it click

Like a residential building: a doorman who questions everyone entering (firewall), a guarded private corridor to your flat (VPN), and a shop on the ground floor whose entrance is on the street rather than inside the building (DMZ). And if the doorman is distracted, your own door is still locked — that is defense in depth.

Ask them these questions

1) Why do we put the public web server in a separate zone rather than inside the internal network?
Expected answer: Because it is more exposed to attack, so if it is breached the attacker does not reach the confidential data inside.

2) Is a firewall alone enough? Why?
Expected answer: No. It is a single point of failure; once an attacker gets past it, everything behind is exposed. That is why measures are layered.

3) What does 'zero trust' mean?
Expected answer: The system trusts nobody automatically, even from inside the network, and verifies every attempt to gain access.

Signs they have not understood

- They think a VPN removes viruses — no, that is the antivirus on the device.
- They read zero trust as 'blocking access' — it means verifying every access.

A 10-minute activity together

Draw a school network on paper: public website + computer lab + student records. Have them place each part and say what protects it, and what would happen if one layer failed.

Suggested study time

45 minutes to study + 25 minutes on questions

2-3 Incident Response and Risk Management

The lesson in plain language

This lesson says that when a breach happens there is an order to follow. The most important thing is to stop the damage spreading first, then remove the cause, and only then restore the work. If you restore before removing the cause, the problem simply returns. There is also a rule for ranking risks: risk = how much damage × how likely it is.

An analogy that makes it click

Like a fire in a flat: first you shut the door on that room so the fire does not spread (containment), then you put out the source (eradication), then you repair and move the furniture back (recovery). Move the furniture back while the fire still burns and you lose it all again.

Ask them these questions

1) Put these in order: recovery — containment — eradication.
Expected answer: Containment → eradication → recovery. This order is the heart of the lesson.

2) A big but rare risk, and a small but frequent one — which comes first?
Expected answer: The words alone are not enough to rank them; it depends on the scores and context. The one that is certainly first is: big × frequent.

3) Is updating software to add features a security incident?
Expected answer: No, that is normal operation. This question is set to test whether they can tell an incident from routine work.

Signs they have not understood

- They start with recovery before removing the cause — the classic mistake here.
- They judge risk by impact alone, without likelihood.

A 10-minute activity together

Give them a scenario: the school's files have been encrypted and someone is demanding a ransom — what is the first step? Have them walk through the six stages out loud. Then ask: what could have prevented the disaster entirely? (Answer: regular backups.)

Suggested study time

35 minutes to study + 20 minutes on questions

3-1 The Overall Structure of Web Applications

The lesson in plain language

This lesson takes apart any website you use into three parts: the screen you see and type into, the hidden part on the server that thinks and decides, and the store where the data is kept. Anything you do travels through all three in order and comes back.

An analogy that makes it click

Like a restaurant: the waiter who takes your order (frontend), the kitchen that prepares it (backend), and the fridge holding the ingredients (database). The waiter alone cannot make you a meal.

Ask them these questions

1) When you type a product name and press search, what happens in order?
Expected answer: Frontend takes the words → sends them to the backend → backend searches the database → data comes back → backend organises it → frontend displays it.

2) A page opened fine but shows no data. Which part is working and which has failed?
Expected answer: The frontend works, because the page displayed; the problem is most likely the backend or the database.

3) 'Storing order history' and 'checking stock' — which part does each?
Expected answer: Storing → the database. Checking stock → the backend.

Signs they have not understood

- They say the backend runs on the browser — no, on the server.
- They mix up backend and database: the backend decides, the database stores.

A 10-minute activity together

Open a shopping site together and run a search. Have them say out loud: which part is working now? Repeat three times with different services (video, banking, delivery).

Suggested study time

35 minutes to study + 20 minutes on questions

3-2 Web Application Communication Methods

The lesson in plain language

This lesson explains how your device talks to the server. Your device sends a 'request' and the server sends back a 'response'. There are two kinds of request: one that fetches data and one that sends data. The reply carries a number telling you whether it worked: 200 fine, 404 page not found, 500 the server itself has a fault.

An analogy that makes it click

Like calling directory enquiries: you ask (the request) and they answer (the response). 'That number does not exist' is like 404; 'the line itself is down' is like 500.

Ask them these questions

1) What is the difference between GET and POST?
Expected answer: GET fetches data from the server (displaying a page, search results); POST sends data to it (logging in, submitting a form).

2) If you see 404 and if you see 500 — whose side is the problem on in each case?
Expected answer: 404: the page you asked for does not exist. 500: the fault is on the server itself, not with you.

3) Why must a login page use https?
Expected answer: Because the password travels across the network, and encryption stops any third party reading it.

Signs they have not understood

- They swap GET and POST — train them with examples, not memorisation.
- They think 500 is the user's mistake — no, it is the server's.

A 10-minute activity together

If there is a browser to hand, open the developer tools (F12), go to the Network tab and refresh any page. They will see the requests and status codes with their own eyes — this fixes the lesson better than any revision.

Suggested study time

35 minutes to study + 20 minutes on questions

3-3 Fundamentals of Frontend Technology

The lesson in plain language

Any web page is made of three things working together: one that sets the structure (headings, paragraphs, images), one that sets the appearance (colours, arrangement, fonts), and one that makes the page respond to you (press a button and something happens).

An analogy that makes it click

Like a house: the bricks and columns (HTML), the paint and tiling (CSS), and the wiring and plumbing that work when you flip a switch (JavaScript). A house without wiring looks fine but does nothing.

Ask them these questions

1) Which one sets the page colour, and which makes the button work?
Expected answer: Colour → CSS. Button → JavaScript. Mixing these up is the most common mistake in this lesson.

2) What is semantic HTML and what is it for?
Expected answer: Using tags whose names carry meaning, such as header and nav. It helps screen readers for blind users understand the page, and helps search engines understand the content.

3) A site looks terrible on a phone — what is it missing?
Expected answer: Responsive design, which makes the layout adjust automatically to any screen size.

Signs they have not understood

- They say CSS adds behavior — no, it only sets the appearance.
- They think responsive design means building a second site for mobile — no, the same page adapts.

A 10-minute activity together

Open any site and ask: if we removed the colours and arrangement, what would be left? (The structure.) And if the buttons stopped working, what has failed? (JavaScript.) That exercise fixes all three roles in minutes.

Suggested study time

40 minutes to study + 20 minutes on questions