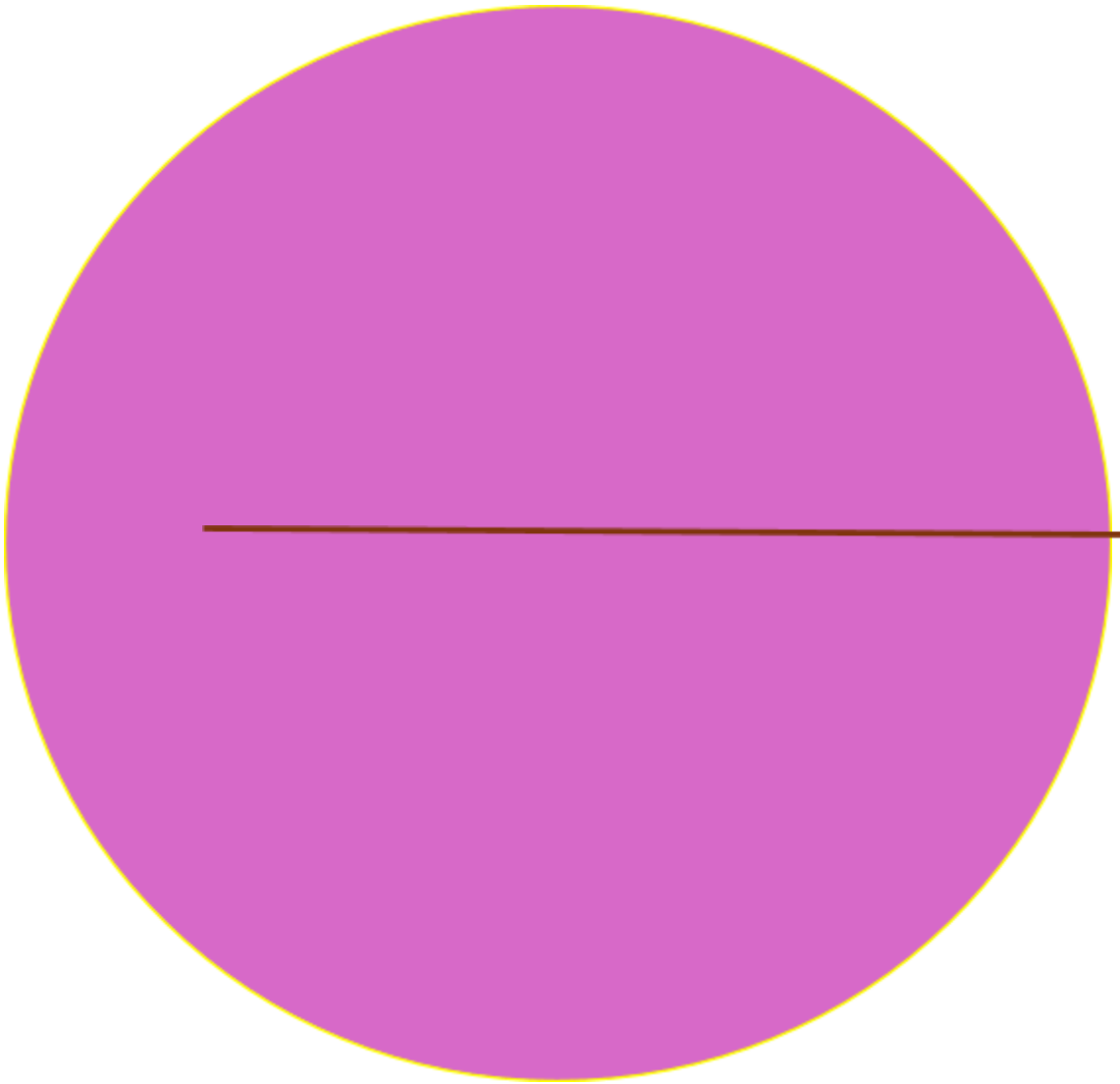
UEAMPUS
STUDY GUIDE



uecampus.com/

First published in 2026 by UE Campus

Unit specifications can be found on the UE Campus Portal: https://uecampus.com/

Contents

Using your Study Guide

Welcome to the study guide, designed to support you in completing your Level 4 Diploma in Information Technology.

This study guide follows the order of the syllabus, which is the basis for your studies. Each chapter starts by listing the syllabus learning outcomes covered and the assessment criteria.

Level 4 Units

Unit Reference	Mandatory Units	Level	TQT	Credit	GLH
L/617/6692	Information Technology and IT Ethics	4	200	20	100
R/617/6693	Mathematics and Statistics for IT	4	200	20	100
Y/617/6694	PC Maintenance and Operating Systems	4	200	20	100
D/617/6695	Computer Graphics Editing and Database Concepts	4	200	20	100
M/617/6698	Web Design 1	4	200	20	100
T/617/6699	Web Programming	4	200	20	100

The study guide includes a number of features to enhance your studies:

📝	**'Over to you:'** activities for you to apply what you have learned.
🌍	**'Industry Insights:'** discover up-to-date trends, expert opinions, and real-world examples from leading organisations in the IT industry.
🧭	**'Did you know?'** highlights interesting facts or surprising information to deepen your understanding of IT topics.
💼	**'Case studies:'** realistic business scenarios to reinforce and test your understanding.
❗	**'Need to know:'** key pieces of information highlighted in the text.

Note: Website addresses current as of March 2026.

Level 4 Information Technology and IT Ethics

About this unit

This unit aims to develop your knowledge and use of information technology, including the use of standard office applications to prepare documents and presentations. This includes computer software and hardware, basic computer operations, application software, operating systems, information systems and IT-related issues in computing.

The unit also seeks to provide you with an awareness of ethical issues essential to an IT professional. This includes ethics in cyberspace, intellectual property, privacy, the issue of security and reliability, how computing affects our health, professional codes of ethics and how IT changes our daily lives.

By the end of this unit, you will have a solid understanding of both the technical foundations of IT and the ethical responsibilities that come with working in the technology sector. These two areas are inseparable in modern professional practice – understanding one without the other leaves a significant gap in your knowledge.

Chapter One – The Applications of Information Technology

Introduction

This chapter examines the applications of information technology across various contexts. You will analyse the uses, strengths and limitations of different categories of hardware and software, explore the growing applications of artificial intelligence, and learn how to produce specifications and presentations for IT applications.

Information technology is now embedded in virtually every aspect of modern life – from the smartphone in your pocket to the cloud infrastructure powering global businesses. Understanding the range and capability of these technologies, as well as their limitations, is fundamental to any career in IT.

On completion of this chapter, you will be able to demonstrate your understanding of the wide range of IT applications and how they can be effectively used in both personal and professional settings.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand the applications of information technology.**

Assessment Criteria

1.1 Analyse the uses, strengths and limitations of different categories of hardware and software.

1.2 Analyse the applications of artificial intelligence (AI).

1.3 Produce a specification of requirements for an application that meets the brief.

1.4 Create and present presentations that demonstrate an application layout using planning tools.

1.1 The uses, strengths and limitations of different categories of hardware and software

📝 Over to you – Video Watch: How Computers Work

Watch this YouTube video:

Title: How Computers Work: What Makes a Computer, a Computer? – Code.org

Duration: 4:12

Link: https://www.youtube.com/watch?v=mCq8-xTH7jA

After watching this video, note down the four key functions of a computer. How do these functions relate to the hardware categories discussed below?

Today's Technologies: Computers, Devices, and the Web

Information technology encompasses the hardware, software, and networks used to process, store, and communicate data. The term covers everything from personal devices such as smartphones and laptops to large-scale enterprise systems including data centres and cloud computing platforms. Understanding the different categories of technology is fundamental to working effectively in any IT-related role.

The rapid pace of technological change means that new categories of devices and software emerge regularly. For example, the Internet of Things (IoT) has created an entirely new class of connected devices – from smart thermostats and wearable fitness trackers to industrial sensors monitoring factory equipment. As an IT professional, you need to understand not just current technologies, but also emerging trends that may reshape the industry.

Hardware

Hardware refers to the physical, tangible components of a computer system. Without hardware, software has nothing to run on. Hardware can be broadly categorised into four types based on function: input, output, processing, and storage.

Input Devices

Input devices allow you to enter data and instructions into a computer. They convert human actions into digital signals the computer can process. Common input devices include:

- Keyboard – the most widely used input device for text entry and commands. Modern keyboards may include programmable keys and backlighting for specialist use.
- Mouse and Trackpad – pointing devices for navigating graphical user interfaces (GUIs). Gaming mice may feature additional programmable buttons and high-precision sensors.
- Scanner – converts physical documents and images into digital format. Flatbed scanners are common in offices, while handheld scanners are used in logistics for barcode reading.

- Microphone – captures audio input, essential for voice recognition, virtual meetings, and podcasting. Modern AI-powered microphones can filter background noise in real time.
- Webcam – captures video input for video conferencing, live streaming, and security surveillance.
- Touchscreen – combines input and output; used extensively on smartphones, tablets, and interactive kiosks.
- Biometric devices – fingerprint scanners, facial recognition cameras, and iris scanners used for authentication and security.

> 🧭 **Did you know?**
>
> The average person touches their smartphone over 2,600 times a day. Touchscreen technology, first developed in the 1960s, has become the dominant input method for mobile devices – replacing physical keyboards entirely on most modern smartphones.

Output Devices

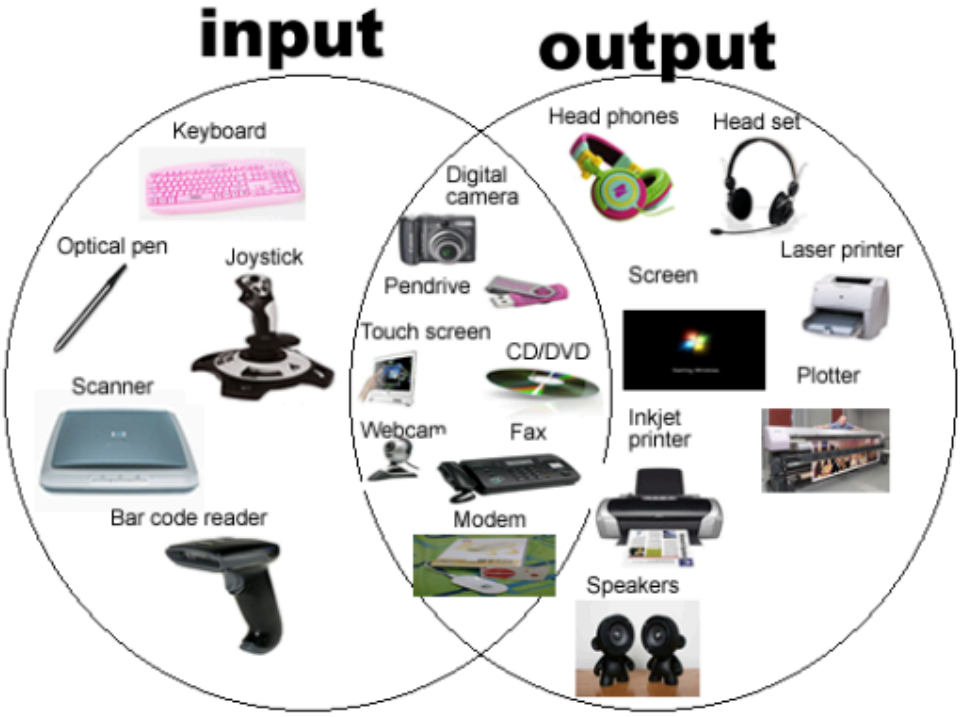
Output devices present processed data in a form that humans can understand. They convert digital signals back into text, images, sound, or physical objects:

- Monitor – the primary visual output device. Modern monitors range from standard LCD displays to ultra-high-definition (4K/8K) screens and curved gaming monitors.
- Printer – produces hard copies of digital documents. Types include inkjet (home use), laser (office use), and 3D printers (manufacturing and prototyping).
- Speakers and Headphones – produce audio output for music, communication, and system notifications.
- Projector – displays output on a large surface, commonly used in presentations, classrooms, and home cinema setups.

Processing Devices

Processing devices are the components that perform calculations and execute instructions. They are the ‘brain’ of the computer:

- Central Processing Unit (CPU) – the primary processor that performs arithmetic, logic, and control operations. CPU performance is measured in clock speed (GHz) and number of cores. Leading manufacturers include Intel and AMD.
- Graphics Processing Unit (GPU) – a specialised processor designed for rendering images, video, and animations. GPUs are also increasingly used for AI and machine learning workloads due to their ability to process thousands of operations simultaneously.
- RAM (Random Access Memory) – temporary, volatile memory that stores data currently being processed. More RAM allows you to run more applications simultaneously without slowing down.



🌍 Industry Insight – The Rise of Cloud Computing

According to Gartner, worldwide end-user spending on public cloud services is forecast to reach over $723 billion in 2025. Companies like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform dominate the market. Cloud computing allows businesses of all sizes to access powerful computing resources on demand, without investing in expensive on-premises hardware. This has fundamentally changed how IT infrastructure is planned, deployed, and managed.

Visit: https://aws.amazon.com/what-is-cloud-computing/ to learn more about how cloud infrastructure works.

Storage Devices

Storage devices retain data permanently (or until deliberately deleted), even when the computer is switched off. The choice of storage depends on factors such as speed, capacity, portability, and cost:

- Hard Disk Drive (HDD) – uses spinning magnetic platters to store data. Offers large capacity at low cost but is slower and more fragile than solid-state alternatives.
- Solid State Drive (SSD) – uses flash memory with no moving parts. Significantly faster, more durable, and energy-efficient than HDDs, though generally more expensive per gigabyte.
- USB Flash Drive – small, portable storage device useful for transferring files between computers. Capacities now range from 8GB to over 1TB.

- Cloud Storage – data stored remotely on servers accessed via the internet. Services such as Google Drive, Microsoft OneDrive, and Dropbox allow you to access your files from any device, anywhere.
- Network Attached Storage (NAS) – a dedicated file storage device connected to a network, commonly used in small businesses for shared file access and automated backups.

🧭 Did you know?

The first commercial hard disk drive, the IBM 350 (1956), stored just 3.75 megabytes of data and was the size of two refrigerators. Today, a microSD card smaller than your fingernail can hold 1 terabyte – that is over 266,000 times the capacity in a fraction of the size.

Software

Software refers to the programs and operating information that instruct hardware on what to do. Without software, hardware is simply an inert collection of components. Software is broadly categorised into two types: system software and application software.

1. System Software

System software manages the computer's hardware resources and provides a platform on which application software runs. It acts as an intermediary between the user and the hardware.

- Operating Systems (OS) – the most important piece of system software. Examples include Microsoft Windows, macOS, Linux, Android, and iOS. The OS manages memory, processes, file systems, security, and provides a graphical or command-line interface for the user.
- Device Drivers – small programs that enable the operating system to communicate with specific hardware components such as printers, graphics cards, and network adapters.
- Utility Software – tools for system maintenance and optimisation, including antivirus programs (e.g. Norton, Kaspersky), disk management tools, backup utilities, and system monitors.
- Firmware – low-level software permanently embedded in hardware devices such as routers, BIOS chips, and embedded systems. Firmware controls how a device operates at the most fundamental level.

📝 Over to you – Video Watch: Operating Systems

Watch this YouTube video:

Title: Operating Systems: Crash Course Computer Science #18

Duration: 13:35

Link: https://www.youtube.com/watch?v=26QPDBe-NB8

After watching, list three key functions of an operating system. How does the OS act as an intermediary between you and the hardware?

2. Application Software

Application software is designed to perform specific tasks for you. Unlike system software, which runs in the background, application software is what you directly interact with:

- Productivity Software – Microsoft Office Suite (Word, Excel, PowerPoint), Google Workspace (Docs, Sheets, Slides). These tools are essential for document creation, data analysis, and presentations.
- Graphics and Design Software – Adobe Photoshop, Illustrator, Canva, Figma. Used for image editing, graphic design, and UI/UX prototyping.
- Web Browsers – Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge. Your gateway to the World Wide Web.
- Communication and Collaboration Software – Microsoft Teams, Zoom, Slack, Google Meet. These tools have become essential for remote and hybrid working.
- Database Management Software – MySQL, Microsoft Access, Oracle Database, MongoDB. Used to store, organise, retrieve, and manage large volumes of structured data.
- Security Software – firewalls, antivirus programs, encryption tools, and VPNs (Virtual Private Networks) that protect systems and data from threats.

Strengths and Limitations of Hardware and Software Categories

Category	Strengths	Limitations
Desktop Computers	Powerful processing; upgradeable; large storage; multiple monitors	Not portable; higher power consumption; requires dedicated space
Laptops	Portable; built-in battery; versatile for work and study	Limited upgrade options; can overheat; smaller screen
Tablets / Smartphones	Highly portable; touchscreen; always connected; app ecosystem	Limited processing power; small screen; less suitable for complex tasks
Cloud Computing	Scalable on demand; accessible anywhere; pay-as-you-go pricing	Requires internet; data security concerns; vendor lock-in risk
Open-source Software	Free to use; customisable; strong community support; transparent code	May lack professional support; compatibility issues; steeper learning curve
Proprietary Software	Professional support; regular updates; polished user interface; integration	Expensive licensing; limited customisation; vendor dependency
IoT Devices	Real-time data collection; automation; improved efficiency	Security vulnerabilities; privacy concerns; interoperability issues

📝 Over to you – Research Activity

Visit the website of a major cloud provider (e.g. AWS, Microsoft Azure, or Google Cloud). Identify three services they offer and explain how a small business might use each one. Write your findings in approximately 300 words.

Connecting and Communicating Online

The internet and the World Wide Web have transformed how we communicate, work, learn, and do business. Understanding how networks operate is fundamental to IT.

A computer network is a group of interconnected devices that share resources and communicate with each other. Networks range from small Local Area Networks (LANs) in a single building to the global Wide Area Network (WAN) that is the internet. Key networking concepts include protocols (rules for communication, such as TCP/IP and HTTP), bandwidth (the capacity of a network connection), and latency (the delay in data transmission).

Wireless technologies, including Wi-Fi, Bluetooth, and 5G mobile networks, have made connectivity ubiquitous. The growth of the Internet of Things (IoT) means that billions of devices – from home appliances to industrial machinery – are now connected to the internet, generating vast quantities of data.

🧭 Did you know?

As of 2025, there are an estimated 18.8 billion IoT devices worldwide – more than double the global population. By 2030, this number is projected to exceed 30 billion. This growth

creates both opportunities (smart cities, precision agriculture, remote healthcare) and challenges (security vulnerabilities, data privacy, electronic waste).

1.2 The applications of artificial intelligence (AI)

Artificial intelligence (AI) refers to the simulation of human intelligence by computer systems. AI technologies are designed to perform tasks that normally require human cognition, such as learning, reasoning, problem-solving, perception, and natural language understanding. AI is no longer a futuristic concept – it is embedded in the products and services you use every day, from the recommendations on your Netflix home screen to the spam filter in your email inbox.

📝 Over to you – Video Watch: Machine Learning & AI

Watch this YouTube video:

Title: Machine Learning & Artificial Intelligence: Crash Course Computer Science #34

Duration: 11:49

Link: https://www.youtube.com/watch?v=z-EtmaFJieY

After watching, explain in your own words: What is the difference between supervised and unsupervised learning? Give one real-world example of each.

Key Areas of AI Application

Machine Learning (ML)

Machine learning is a subset of AI that enables computers to learn from data and improve their performance over time without being explicitly programmed for every scenario. ML algorithms identify patterns in data and use those patterns to make predictions or decisions. There are three main types of machine learning:

- Supervised learning – the algorithm learns from labelled training data (e.g. classifying emails as spam or not spam based on thousands of previously labelled examples).
- Unsupervised learning – the algorithm finds hidden patterns in unlabelled data (e.g. grouping customers into segments based on purchasing behaviour).
- Reinforcement learning – the algorithm learns through trial and error, receiving rewards for correct actions (e.g. training a robot to navigate a maze or teaching a game-playing AI).

Applications of ML include recommendation systems (Netflix, Spotify, Amazon), fraud detection in banking, medical diagnosis, predictive maintenance in manufacturing, and autonomous vehicles.

Natural Language Processing (NLP)

NLP enables computers to understand, interpret, and generate human language. This is the technology behind voice assistants like Siri and Alexa, language translation services like Google Translate, chatbots for customer service, and sentiment analysis tools that help businesses understand customer opinions from social media posts and reviews. Large

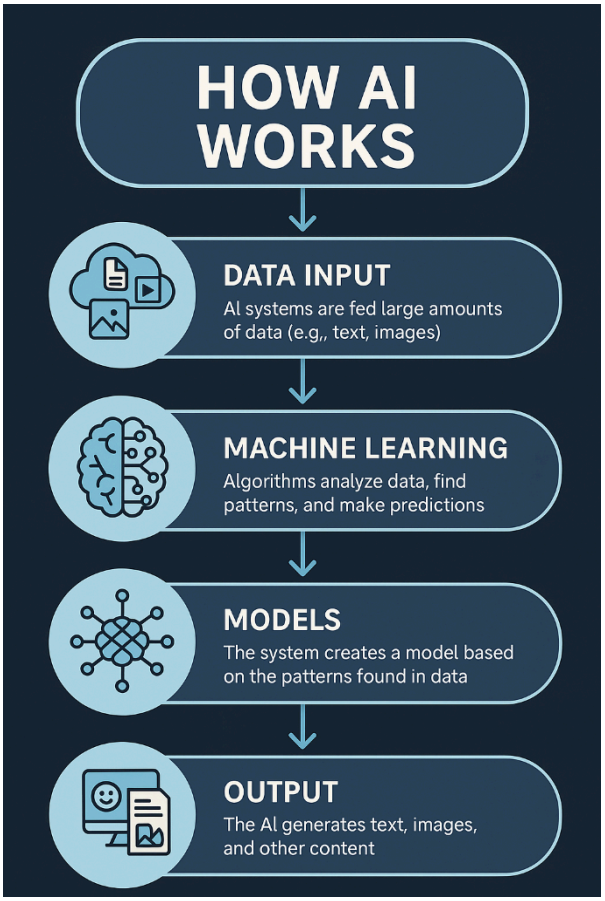
language models (LLMs) such as GPT-4 and Claude represent the latest advances in NLP, capable of generating human-like text, summarising documents, writing code, and answering complex questions.

Computer Vision

Computer vision enables machines to interpret and make decisions based on visual information from the world. Applications include facial recognition (used in smartphone unlocking and security systems), autonomous vehicles (which must interpret road conditions in real time), medical image analysis (detecting tumours in X-rays and MRI scans), quality control in manufacturing (identifying defective products on assembly lines), and augmented reality (AR) applications.

Robotics and Automation

AI-powered robots and automated systems are transforming industries. In manufacturing, robots perform repetitive assembly tasks with precision. In logistics, companies like Amazon use AI-driven robots in their fulfilment centres to pick, pack, and ship products. In healthcare, surgical robots assist surgeons with minimally invasive procedures. In agriculture, autonomous drones and robots monitor crops and apply treatments precisely where needed.



Expert Systems

Expert systems are AI programs that replicate the decision-making abilities of a human expert in a specific domain. They use a knowledge base (a collection of facts and rules) and an inference engine (which applies logical rules to the knowledge base) to solve complex problems. Expert systems are used in medical diagnosis, financial planning, technical troubleshooting, and legal analysis.

🌍 Industry Insight – AI in Healthcare

AI is transforming healthcare at an extraordinary pace. Google's DeepMind has developed AI systems that can detect over 50 eye diseases from retinal scans with accuracy matching leading ophthalmologists. In drug discovery, AI algorithms can analyse millions of molecular combinations to identify potential new medicines in a fraction of the time traditional methods require. The NHS is piloting AI tools for early cancer detection, using machine learning to analyse mammograms and identify signs of breast cancer that human radiologists might miss.

Read more: BBC News – 'AI detects cancer earlier than doctors': https://www.bbc.co.uk/news/health

📝 Over to you – Blog and Research Activity

Visit the MIT Technology Review website (https://www.technologyreview.com/) and search for a recent article about AI. Read the article and write a 200-word summary answering: What AI technology is discussed? What problem does it solve? What are the potential benefits and risks?

🧭 Did you know?

ChatGPT, developed by OpenAI, reached 100 million monthly active users within two months of its launch in November 2022 – making it the fastest-growing consumer application in history at that time. This growth highlighted both the enormous potential and the ethical concerns surrounding generative AI.

1.3 Producing a specification of requirements for an application that meets the brief

A specification of requirements (often called a Software Requirements Specification or SRS) is a detailed document that outlines what a software application or system must do. It serves as a blueprint for developers and stakeholders, ensuring that the final product meets its intended purpose and that everyone involved shares the same understanding of the project.

Writing a clear and comprehensive requirements specification is one of the most important stages in any IT project. Research consistently shows that errors in requirements are the most common and most expensive cause of project failure. A well-written specification reduces misunderstandings, prevents scope creep, and provides a benchmark against which the finished product can be evaluated.

Key Components of a Requirements Specification

Functional Requirements

Functional requirements describe what the system should do – the specific features and functions it must provide. These are expressed as concrete, testable statements. Examples include: 'The system shall allow users to create an account using an email address and password', 'The system shall generate a monthly sales report in PDF format', and 'The system shall send an email notification when an order is dispatched'.

Non-Functional Requirements

Non-functional requirements specify how the system should perform rather than what it should do. They define quality attributes such as performance ('The system shall load any page within 2 seconds'), reliability ('The system shall have 99.9% uptime'), security ('All user passwords shall be stored using bcrypt hashing'), usability ('The system shall be accessible to users with visual impairments, compliant with WCAG 2.1 AA standards'), and scalability ('The system shall support up to 10,000 concurrent users').

User Requirements

User requirements describe the system from the perspective of the end user. They are often written as 'user stories' in agile development – for example: 'As a student, I want to view my timetable on my phone so that I can check my schedule between classes.' User requirements ensure that the system is designed with the people who will actually use it in mind.

System Requirements

System requirements detail the technical environment needed to run the application. This includes the hardware platform (e.g. minimum RAM, processor speed), software

dependencies (e.g. operating system version, database server), network requirements (e.g. bandwidth, VPN access), and any third-party integrations (e.g. payment gateways, APIs).

Constraints

Constraints identify the boundaries within which the project must operate. These include budget limitations, delivery timelines, regulatory compliance (e.g. GDPR, PCI-DSS for payment processing), technology restrictions, and organisational policies.

💼 Case Study – Building a Student Management System

A college needs a new student management system. The project team has identified the following requirements: the system must allow staff to register students, record and calculate grades, generate attendance reports, and integrate with the existing finance system for fee payments. Non-functional requirements include 99.9% availability during term time, support for 500 concurrent users, GDPR compliance, and full mobile responsiveness.

Task: Draft a requirements specification for a mobile app that helps university students manage their study timetable. Include at least three functional requirements, three non-functional requirements, two user stories, and two constraints. Present your work in a structured document.

1.4 Creating and presenting presentations that demonstrate an application layout using planning tools

Creating effective presentations is a key professional skill for IT practitioners. Whether you are pitching a new application to stakeholders, presenting a project update to your team, or demonstrating a prototype to clients, the ability to communicate technical ideas clearly and visually is invaluable.

When demonstrating an application layout, planning tools help you organise your ideas, visualise the user experience, and communicate your design decisions to both technical and non-technical audiences.

Planning Tools for Application Design

- Wireframes – simple, low-fidelity sketches or digital mockups showing the layout and structure of an application's screens without detailed design elements. Tools: Balsamiq, Figma, Adobe XD.
- Prototypes – interactive, higher-fidelity representations of the application that simulate user interactions. Prototypes allow stakeholders to 'click through' the application before development begins. Tools: Figma, InVision, Axure.
- Flowcharts – diagrams that represent the flow of a process or system, showing steps, decision points, and outcomes. Essential for mapping user journeys and system logic. Tools: Lucidchart, draw.io, Microsoft Visio.
- Storyboards – visual narratives showing how a user will interact with an application, screen by screen, in sequence.
- Gantt Charts – project management tools showing tasks, durations, milestones, and dependencies on a timeline. Tools: Microsoft Project, Trello (with timeline view), Asana.
- Mind Maps – visual brainstorming tools for organising ideas hierarchically. Useful for the early stages of planning when exploring features and requirements. Tools: MindMeister, XMind.

📝 Over to you – Video Watch: UI/UX Design Fundamentals

Watch this YouTube video:

Title: The 2024 Beginner's Guide to UX Design – DesignCourse

Duration: 26:14

Link: https://www.youtube.com/watch?v=uL2ZB7XXIgg

After watching, identify three principles of good UI design. How would you apply these when creating wireframes for a mobile application?

Microsoft Office PowerPoint

Microsoft PowerPoint remains the industry standard for creating professional presentations. However, alternatives such as Google Slides, Apple Keynote, and Canva Presentations are also widely used. Regardless of the tool, effective presentation skills follow the same principles.

Best Practices for IT Presentations

- Keep slides clear and uncluttered – follow the 6×6 rule (no more than 6 bullet points per slide, no more than 6 words per bullet).
- Use visuals generously – wireframe screenshots, flowcharts, system architecture diagrams, and mockups are far more effective than text-heavy slides.
- Tell a story – structure your presentation with a clear beginning (the problem), middle (your solution), and end (expected outcomes and next steps).
- Include a live demonstration or walkthrough – showing a working prototype or clickable wireframe engages the audience far more than static slides.
- Prepare speaker notes – to ensure key points are covered without reading directly from slides. Notes also help if someone else needs to deliver your presentation.
- Consider your audience – a presentation to developers will differ significantly from one aimed at business stakeholders or end users. Tailor your language and level of technical detail accordingly.

📝 Over to you – Presentation Task

Using Microsoft PowerPoint (or Google Slides), create a 10-slide presentation that demonstrates the layout and features of a proposed mobile application of your choice. You must include at least two wireframe mockups, one flowchart showing the user journey, and one slide summarising the technical requirements. Include speaker notes on every slide explaining your design decisions.

Reading List

- Freund, S.M., Frydenberg, M., Last, M.Z. & Pratt, P.J. (2023). *Discovering Computers 2023: Digital Technology, Data, and Devices.* Boston: Cengage Learning.
- Gallaugher, J. (2024). *Information Systems: A Manager's Guide to Harnessing Technology.* 10th edn. Boston: FlatWorld.
- Schmidt, C. (2025). *Complete A+ Guide to IT Hardware and Software: CompTIA A+ Core 1 and Core 2 Exams.* Hoboken, NJ: Pearson.
- Tanenbaum, A.S. & Bos, H. (2023). *Modern Operating Systems.* 5th edn. Harlow: Pearson.
- Torralba, A., Isola, P. & Freeman, W.T. (2024). *Foundations of Computer Vision.* Cambridge, MA: MIT Press.
- Wallace, P. (2024). *Introduction to Information Systems.* 5th edn. Hoboken, NJ: Pearson.

Summary

In this chapter, you have explored the fundamental categories of hardware and software, understanding their uses, strengths, and limitations in professional and personal contexts. You have analysed the growing applications of artificial intelligence across multiple industries, from healthcare to logistics. You have also learned how to produce a well-structured requirements specification and how to use planning tools to create effective presentations demonstrating application layouts. These skills form the foundation of IT professional practice and will be built upon throughout your programme.

Chapter Two – The Ethics Involved in Information Technology

Introduction

This chapter explores the ethical dimensions of information technology. You will examine the nature of IT ethics, the relationship between ethics, morality and society, and why information technology gives rise to unique ethical dilemmas not found in other fields. You will also evaluate key issues relating to IT ethics, including privacy, intellectual property, security, reliability, professional responsibility, and the impact of IT on work and wealth.

Ethics is not an abstract academic exercise – it is central to your daily professional practice as an IT professional. Every decision you make, from how you handle user data to how you design algorithms, has ethical implications. The technologies you build and manage affect the lives of real people, and with that power comes significant responsibility.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand the ethics involved in information technology.**

Assessment Criteria

2.1 Analyse the nature of information technology ethics and its application to IT.

2.2 Analyse the analogy that relates ethics, morality and society.

2.3 Assess how and why information technology gives rise to ethical dilemmas not present in other technologies.

2.4 Evaluate the issues relating to IT ethics, justifying their conclusions.

2.1 The nature of information technology ethics and its application to IT

Ethics is the branch of philosophy that deals with questions of right and wrong, moral duty, and obligation. In the context of information technology, IT ethics examines the moral issues that arise from the development, deployment, use, and management of technology. It asks questions such as: Who is responsible when an AI system makes a harmful decision? Is it acceptable for an employer to monitor employees' emails? Should facial recognition technology be used in public spaces?

📝 Over to you – Video Watch: Cybersecurity and Ethics

Watch this YouTube video:

Title: Cybersecurity: Crash Course Computer Science #31

Duration: 12:30

Link: https://www.youtube.com/watch?v=bPVaOlJ6ln0

After watching, reflect: What ethical responsibilities do you think cybersecurity professionals have? Write down three ethical dilemmas a cybersecurity professional might face.

Ethical Frameworks

To analyse ethical issues systematically, it helps to understand the main philosophical frameworks. Each framework offers a different lens through which to evaluate moral questions:

Utilitarianism (Consequentialism)

Actions are judged by their outcomes – the morally right action is the one that produces the greatest good for the greatest number of people. For example, a utilitarian might argue that sharing anonymised health data for medical research is ethical because the benefit to society outweighs the minor privacy risk to individuals.

Deontological Ethics (Kantianism)

Actions are judged by whether they follow established moral rules or duties, regardless of their outcomes. From a deontological perspective, collecting user data without informed consent is always wrong, even if it leads to beneficial outcomes, because it violates the individual's right to privacy and autonomy.

Virtue Ethics

Focuses on the character and intentions of the moral agent rather than the specific act or its consequences. A virtue ethicist would ask: 'What would a person of good character do in this situation?' This framework emphasises traits such as honesty, integrity, fairness, and compassion.

Social Contract Theory

Ethical behaviour is based on an implicit agreement among members of society. We agree to follow certain rules (e.g. not stealing, respecting privacy) in exchange for the benefits of living in an ordered society. In IT, this is reflected in terms of service agreements, acceptable use policies, and professional codes of conduct.

🧭 Did you know?

The Computer Ethics Institute published 'The Ten Commandments of Computer Ethics' in 1992. They include principles such as 'Thou shalt not use a computer to harm other people', 'Thou shalt not snoop around in other people's files', and 'Thou shalt think about the social consequences of the program you are writing.' While the language is dated, the principles remain highly relevant today.

How Ethics Applies to IT in Practice

As an IT professional, you will face ethical challenges regularly. Key areas where ethics intersects with IT practice include:

- Data collection and use – How organisations gather, store, analyse, and share personal data. Are users fully informed? Is consent meaningful?
- Software development – Ensuring software is designed responsibly, free from harmful bias, accessible to all users, and adequately tested before release.
- Cybersecurity – Balancing the need to protect systems from attacks with respect for user privacy. Is it ethical to monitor all employee communications for security purposes?
- AI and automation – Addressing questions of accountability (who is responsible when an autonomous car crashes?), transparency (can users understand how an AI made a decision?), and fairness (does the algorithm discriminate against certain groups?).
- Environmental impact – The carbon footprint of data centres, the growing problem of electronic waste, and the ethical responsibility to develop sustainable technology.

📝 Over to you – Ethical Scenarios

Read the following scenario and apply two different ethical frameworks to analyse it:

Scenario: A software company discovers a security vulnerability in its widely used messaging app. Fixing the vulnerability will take two weeks. Should the company inform users immediately (risking exploitation by hackers in the meantime) or wait until the fix is ready?

Analyse this using (1) utilitarianism and (2) deontological ethics. Which approach do you find more convincing, and why?

2.2 The analogy relating ethics, morality and society

Ethics, morality, and society are deeply interconnected concepts. Understanding their relationship is essential for you as an IT professional, because the technologies you create and manage operate within a complex social and moral context.

Morality

Morality refers to your personal beliefs about right and wrong, often shaped by your culture, religion, family, and life experiences. Moral beliefs are deeply held and can vary significantly between individuals and communities. For example, attitudes towards online privacy differ markedly between cultures – what is considered an acceptable level of government surveillance in one country may be viewed as a fundamental violation of rights in another.

Ethics

Ethics provides a more systematic, structured framework for evaluating moral questions. While morality is personal, ethics seeks to establish principles that can be applied consistently and defended through rational argument. Professional ethics, such as those codified by the BCS (British Computer Society) or the ACM (Association for Computing Machinery), represent agreed standards of behaviour for IT professionals.

Society

Society establishes norms, laws, and expectations that reflect collective moral values and ethical standards. Laws such as the UK Data Protection Act 2018 and the EU's General Data Protection Regulation (GDPR) translate ethical principles about privacy into enforceable legal requirements. However, law and ethics do not always align – something can be legal but unethical, or illegal but morally justifiable.

The interplay between these three concepts is particularly important in IT. Social media platforms, for instance, may legally collect vast amounts of user data under their terms of service, but many argue this practice is ethically questionable when users do not fully understand what they are consenting to. Similarly, algorithmic decision-making in areas such as criminal justice, hiring, and credit scoring raises fundamental questions about fairness that cannot be resolved by technology alone – they require moral reflection and societal debate.

🌍 Industry Insight – The Cambridge Analytica Scandal

In 2018, it was revealed that the political consulting firm Cambridge Analytica had harvested the personal data of up to 87 million Facebook users without their explicit consent, using it to target political advertising during the 2016 US presidential election and the Brexit referendum. The data was collected through a personality quiz app that also harvested the data of users' friends. While Facebook's terms of service technically permitted this data sharing at the time, the incident was widely condemned as a fundamental breach of trust and ethics. It led to regulatory investigations, a $5 billion fine

for Facebook from the US Federal Trade Commission, and accelerated global efforts to strengthen data protection laws.

Read more: The Guardian – The Cambridge Analytica Files: https://www.theguardian.com/news/series/cambridge-analytica-files

📝 Over to you – Reflection Activity

Consider the following scenario: A social media company uses AI to personalise your news feed, showing you content that keeps you engaged for longer. Research shows this approach can create 'filter bubbles' that reinforce existing beliefs and contribute to political polarisation.

Discuss: Is this practice ethical? How do morality (your personal view), ethics (systematic analysis), and society (laws and norms) intersect in this scenario? What changes would you recommend? Write approximately 300 words.

2.3 How and why information technology gives rise to ethical dilemmas not present in other technologies

Information technology creates unique ethical challenges that are not found in traditional technologies such as the printing press, the telephone, or the internal combustion engine. While all technologies raise ethical questions, several characteristics of IT make its ethical landscape particularly complex and urgent.

📝 Over to you – Video Watch: Hackers & Cyber Attacks

Watch this YouTube video:

Title: Hackers & Cyber Attacks: Crash Course Computer Science #32

Duration: 11:52

Link: https://www.youtube.com/watch?v=_GzE99AmAQU

After watching, identify three types of cyber attack discussed. For each, explain the ethical issues involved from the perspective of both the attacker and the defender.

1. Speed and Scale

Digital actions can affect millions of people in seconds. A single data breach can expose the personal records of millions of individuals simultaneously. Misinformation can spread globally within hours through social media. An algorithmic change by a search engine or social platform can instantly alter what billions of people see and believe. No previous technology has operated at this speed and scale.

2. Invisibility

Many IT processes are invisible to the people they affect. Algorithms that determine what content you see on social media, how your credit score is calculated, whether your job application is shortlisted, or how your insurance premium is set operate behind the scenes, often with no transparency. This 'invisibility factor', as described by James Moor, makes IT uniquely challenging from an ethical perspective because people cannot question or challenge processes they do not know exist.

3. Reproducibility

Digital content can be copied perfectly and distributed infinitely at virtually no cost. A photograph, a song, a software program, or an entire database can be duplicated millions of times with no loss of quality. This raises profound questions about intellectual property, copyright, the value of creative work, and the economics of the digital age. It also makes it extremely easy to spread pirated software, counterfeit media, and stolen data.

4. Permanence

Digital information is extraordinarily difficult to erase completely. Data stored online can persist indefinitely, replicated across multiple servers and cached by search engines. A

photograph posted on social media, a careless comment, or a piece of personal data shared with a third party may never truly disappear. This raises serious concerns about the right to be forgotten, the long-term consequences of digital footprints, and the ability of individuals to move on from past mistakes.

5. Anonymity

The internet allows users to interact anonymously or pseudonymously. This can facilitate both positive outcomes (whistleblowing, political dissent in authoritarian regimes, support for sensitive health conditions) and deeply negative ones (cyberbullying, online fraud, radicalisation, the distribution of illegal content). The tension between protecting anonymity as a form of free expression and preventing its abuse is one of the defining ethical challenges of the digital age.

6. Automation and Algorithmic Bias

Automated decision-making systems can embed and amplify existing societal biases. If an AI hiring tool is trained on historical data from a company that predominantly hired men, it may learn to penalise female applicants – not through deliberate programming, but through patterns in the data. Similarly, predictive policing algorithms have been shown to disproportionately target minority communities. These issues represent a category of ethical dilemma that simply did not exist before the advent of AI and big data.

🧭 Did you know?

The European Union's General Data Protection Regulation (GDPR), implemented in 2018, was one of the first comprehensive legal frameworks to address the unique ethical challenges posed by digital technologies. It gives individuals the right to access, correct, and delete their personal data held by organisations. Under GDPR, organisations can face fines of up to €20 million or 4% of their annual global turnover for serious violations.

📝 Over to you – News Analysis

Search a reputable news source (e.g. BBC News, The Guardian, Wired, or Ars Technica) for a recent story about a data breach, AI bias, or online privacy issue. Write a 250-word analysis identifying: (1) which of the six characteristics above contributed to the ethical dilemma, (2) who was affected and how, and (3) what could have been done differently. Include a full reference to the article.

2.4 Issues relating to IT ethics

Several key issues define the ethical landscape of information technology. As an IT professional, you must understand and critically engage with these issues to act responsibly and ethically in your role. This section examines the most significant areas of IT ethics in detail.

Intellectual Property

Intellectual property (IP) refers to creations of the mind – inventions, literary and artistic works, designs, symbols, names, and software – protected by law through patents, copyrights, and trademarks. In IT, intellectual property issues are particularly complex because digital content is so easy to copy and distribute.

Key IP issues in IT include software piracy (the unauthorised copying and distribution of commercial software), open-source licensing (which allows software to be freely used, modified, and shared under specific conditions), patent disputes (particularly in areas such as smartphone technology, where overlapping patents lead to costly legal battles), and the challenge of protecting digital content (music, film, books, photographs) in an age when perfect copies can be made instantly.

The tension between protecting the rights of creators and ensuring broad access to knowledge and innovation is one of the central ethical debates in IT. Organisations like Creative Commons offer alternative licensing models that try to balance these competing interests.

Information Privacy

Privacy in the digital age concerns the collection, storage, use, and sharing of personal information. Every time you browse the web, use a mobile app, make an online purchase, or interact with a smart device, you generate data that can be collected, analysed, and potentially monetised.

Key privacy principles include: informed consent (you should know what data is being collected and why), data minimisation (organisations should collect only the data they genuinely need), purpose limitation (data should only be used for the purpose it was collected for), and the right to be forgotten (you should be able to request that your personal data be deleted).

Regulations such as the EU's GDPR and the UK Data Protection Act 2018 establish legal frameworks for protecting personal data. However, the pace of technological change often outstrips the ability of legislation to keep up. Emerging technologies such as facial recognition, smart home devices, and generative AI raise new privacy challenges that existing laws may not fully address.

🌍 Industry Insight – Surveillance Capitalism

In her influential book 'The Age of Surveillance Capitalism' (2019), Harvard professor Shoshana Zuboff argues that major technology companies have created a new economic system in which human experience is treated as free raw material to be translated into behavioural data. This data is then used to predict and influence your behaviour, primarily for the benefit of advertisers. Zuboff argues that this represents a fundamental threat to individual autonomy and democracy.

Read more: https://shoshanazuboff.com/book/about/

Computer and Network Security

Security is both a technical and ethical issue. IT professionals have a moral responsibility to protect systems from unauthorised access, malware, data breaches, and cyberattacks. However, security measures must be balanced against other values, including user convenience, privacy, and civil liberties.

Ethical dimensions of cybersecurity include: the ethics of surveillance and monitoring (is it acceptable for an employer to read employees' emails?), responsible vulnerability disclosure (should a researcher who discovers a software vulnerability inform the vendor privately, or publicise it to pressure a faster fix?), the ethics of 'hacking back' (should organisations be allowed to retaliate against attackers?), and the challenge of balancing national security with individual privacy rights.

📝 Over to you – Video Watch: Cryptography

Watch this YouTube video:

Title: Cryptography: Crash Course Computer Science #33

Duration: 12:32

Link: https://www.youtube.com/watch?v=jhXCTbFnK8o

After watching, explain why encryption is important for both security and privacy. Can you think of a situation where strong encryption might create an ethical dilemma (e.g. for law enforcement)?

Computer Reliability

As society becomes increasingly dependent on computer systems for critical functions – healthcare, transportation, financial services, energy infrastructure, defence – the reliability of these systems becomes an ethical concern of the highest importance. Software bugs, system failures, and inadequate testing can have consequences ranging from financial losses to serious injury or loss of life.

Notable examples include the Boeing 737 MAX crashes (2018–2019), where flawed software in the aircraft's automated flight control system contributed to two fatal accidents killing 346 people. Investigations revealed that software was inadequately tested, and pilots

were not fully informed about the system's behaviour. This case powerfully illustrates the ethical responsibility of IT professionals to ensure that safety-critical systems are thoroughly designed, tested, and documented.

🧭 Did you know?

The Therac-25 radiation therapy machine, used in the 1980s, caused the deaths of at least three patients and seriously injured several others due to software bugs that allowed the machine to deliver massive overdoses of radiation. The case is one of the most studied examples in software engineering ethics and demonstrates the life-and-death consequences of inadequate software testing and safety procedures.

Professional Ethics

Professional codes of ethics provide guidelines for responsible behaviour in the IT profession. The two most widely recognised codes are published by the BCS (British Computer Society) and the ACM (Association for Computing Machinery).

The BCS Code of Conduct requires members to: have due regard for public health, privacy, security, and wellbeing of others and the environment; exercise professional responsibility with integrity; act with competence and not claim any level of competence they do not possess; and comply with relevant authority while also accepting personal responsibility for their work.

The ACM Code of Ethics includes principles such as: contribute to society and to human well-being; avoid harm; be honest and trustworthy; be fair and take action not to discriminate; respect the work required to produce new ideas, inventions, creative works, and computing artefacts; respect privacy; and honour confidentiality.

📝 Over to you – Code of Ethics Comparison

Visit the BCS Code of Conduct (https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/) and the ACM Code of Ethics (https://www.acm.org/code-of-ethics). Compare the two codes by identifying: (1) three principles they share, (2) any differences in emphasis, and (3) one real-world scenario where a principle from either code would guide your decision-making. Write approximately 400 words.

Work and Wealth

Information technology has fundamentally transformed the world of work, creating entirely new industries and job roles while displacing or automating others. The economic and social implications of this transformation raise important ethical questions.

The digital divide – the gap between those who have access to modern information technology and those who do not – remains a significant global challenge. Access to

technology, digital literacy, and reliable internet connectivity are increasingly prerequisites for participation in education, employment, and civic life. Those without access are at a growing disadvantage.

The rise of the gig economy (platforms like Uber, Deliveroo, and Fiverr) has created flexible work opportunities but also raised concerns about workers' rights, job security, and the classification of workers as 'independent contractors' rather than employees. AI and automation threaten to displace millions of jobs in areas such as manufacturing, customer service, data entry, and even professional services like law and accounting. The ethical question is not whether technological progress should continue, but how its benefits and costs should be distributed fairly across society.

💼 Case Study – Data Breach at a Healthcare Provider

A healthcare provider suffers a ransomware attack that encrypts the medical records of 50,000 patients and demands payment in cryptocurrency. An investigation reveals that the organisation had failed to implement basic security measures, including encryption of data at rest, regular software patching, multi-factor authentication for staff, and regular backup testing. Some patients' sensitive medical information is subsequently published on the dark web.

Task: Evaluate the ethical issues raised by this scenario using at least two ethical frameworks. Consider the responsibilities of the IT department, senior management, individual employees, and the attackers. What measures should have been in place to prevent this breach? Who bears the greatest moral responsibility? Write approximately 500 words.

Reading List

- Boddington, P. (2023). *AI Ethics: A Textbook.* Cham: Springer.
- Floridi, L. (2023). *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities.* Oxford: Oxford University Press.
- Liao, S.M. (ed.) (2023). *Ethics of Artificial Intelligence.* New York: Oxford University Press.
- Quinn, M.J. (2024). *Ethics for the Information Age.* 9th edn. Hoboken, NJ: Pearson.
- Spinello, R.A. (2024). *Cyberethics: Morality and Law in Cyberspace.* 7th edn. Burlington, MA: Jones & Bartlett Learning.
- Tavani, H.T. (2022). *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing.* 6th edn. Hoboken, NJ: Wiley.

Summary

In this chapter, you have explored the nature of IT ethics and how ethical frameworks – including utilitarianism, deontological ethics, virtue ethics, and social contract theory – can be applied to real-world technology dilemmas. You have examined the relationship between ethics, morality, and society, and analysed why information technology creates unique ethical challenges not present in other technologies, including issues of speed and scale, invisibility, reproducibility, permanence, anonymity, and algorithmic bias. You have also critically evaluated key issues including intellectual property, information privacy, computer and network security, system reliability, professional ethics, and the impact of IT on work and wealth.

These ethical considerations are not separate from your technical skills – they are integral to them. As you progress through your career in IT, you will be called upon to make decisions that balance technical capability with moral responsibility. The frameworks, case studies, and critical thinking skills developed in this chapter will serve you well in navigating those challenges.

Glossary

Word / Term	Explanation
Algorithm	A step-by-step procedure or set of rules for solving a problem or completing a task, often implemented in software.
Artificial Intelligence (AI)	The simulation of human intelligence by computer systems, including learning, reasoning, and self-correction.
Algorithmic Bias	Systematic errors in AI systems that produce unfair outcomes, often reflecting existing societal prejudices in training data.
Cloud Computing	Delivery of computing services (storage, processing, software) over the internet on a pay-as-you-go basis.
CPU	Central Processing Unit; the primary component of a computer that executes instructions and performs calculations.
Cybersecurity	The practice of protecting computer systems, networks, and data from digital attacks, unauthorised access, and damage.
Data Breach	An incident in which unauthorised individuals gain access to confidential or protected data.
Deontological Ethics	An ethical framework that judges actions based on rules and duties rather than outcomes.
Digital Divide	The gap between those who have effective access to digital technology and those who do not.
Encryption	The process of converting data into a coded format to prevent unauthorised access.
Firmware	Low-level software permanently embedded in hardware devices that controls how the device operates.
GDPR	General Data Protection Regulation; EU legislation governing the collection, use, and protection of personal data.
GPU	Graphics Processing Unit; a specialised processor optimised for rendering images, video, and parallel computations.
Hardware	The physical, tangible components of a computer system.
Intellectual Property	Creations of the mind (inventions, literary works, software) protected by law through patents, copyrights, and trademarks.
Internet of Things (IoT)	A network of physical devices embedded with sensors, software, and connectivity, enabling them to collect and exchange data.
Machine Learning	A subset of AI where systems learn from data and improve their performance without being explicitly programmed.
Malware	Malicious software designed to damage, disrupt, or gain unauthorised access to a computer system.
NLP	Natural Language Processing; the ability of computers to understand, interpret, and generate human language.
Open Source	Software whose source code is freely available for use, modification, and distribution under specific licence terms.
Operating System	System software that manages hardware resources and provides services for application software (e.g. Windows, macOS, Linux).

Phishing	A cyberattack that uses fraudulent communications (often emails) to trick individuals into revealing sensitive information.
Privacy	The right of individuals to control how their personal information is collected, used, and shared.
RAM	Random Access Memory; volatile temporary storage used for data and programs currently in use.
Ransomware	A type of malware that encrypts a victim's data and demands payment for the decryption key.
Software	Programs, applications, and operating information used by a computer to perform tasks.
SSD	Solid State Drive; a storage device using flash memory, offering faster speeds and greater durability than traditional hard drives.
Utilitarianism	An ethical theory that judges actions by their consequences, aiming to produce the greatest good for the greatest number.
Virtue Ethics	An ethical framework that focuses on the character and intentions of the moral agent rather than specific acts or outcomes.
Wireframe	A simple visual guide showing the skeletal layout and structure of an application or website interface.

MCQs and True & False Questions (self-assessment)

True or False Questions

1. Hardware refers to the software programs used on a computer.
2. An operating system is an example of system software.
3. AI can only be used in the technology industry.
4. A requirements specification outlines what a system must do.
5. Non-functional requirements describe how the system should perform.
6. Wireframes show the detailed final design of an application.
7. Ethics examines questions of right and wrong.
8. Morality and ethics are exactly the same thing.
9. GDPR gives individuals the right to access their personal data.
10. Intellectual property only applies to physical inventions.
11. Anonymity on the internet only has negative consequences.
12. Professional codes of ethics guide responsible behaviour in IT.
13. Software piracy is an example of an intellectual property issue.
14. Computer reliability is only a technical concern, not an ethical one.
15. The digital divide refers to unequal access to technology.
16. Encryption protects data by converting it into unreadable code.
17. Phishing is a legitimate form of marketing communication.
18. Cloud storage eliminates all security risks.
19. AI systems can sometimes reflect the biases present in their training data.
20. The BCS Code of Conduct applies only to software developers.

Multiple Choice Questions

1. Which of the following is an input device?

A. Monitor

B. Printer

C. Keyboard

D. Speaker

2. System software includes:

A. Web browsers

B. Operating systems

C. Social media apps

D. Games

3. Which type of storage uses flash memory?

A. HDD

B. CD-ROM

C. SSD

D. Floppy disk

4. AI that enables machines to learn from data is called:

A. Robotics

B. Machine learning

C. Cloud computing

D. Encryption

5. A wireframe is best described as:

A. A final application design

B. A simple layout showing structure

C. A project management tool

D. A type of programming language

6. Which planning tool shows a project timeline with tasks and dependencies?

A. Wireframe

B. Mind map

C. Gantt chart

D. Flowchart

7. Utilitarianism judges actions based on:

A. Rules and duties

B. Character of the person

C. Outcomes and consequences

D. Social contracts

8. GDPR stands for:

A. Global Data Privacy Regulation

B. General Data Protection Regulation

C. General Digital Privacy Rules

D. Global Digital Protection Regulation

9. Which characteristic of IT allows digital content to be copied perfectly?

A. Invisibility

B. Permanence

C. Reproducibility

D. Anonymity

10. The BCS is:

A. A software company

B. A hardware manufacturer

C. The British Computer Society

D. A government agency

11. Which of the following is a non-functional requirement?

A. User login feature

B. Report generation

C. System response time under 2 seconds

D. Data entry form

12. NLP stands for:

A. Network Layer Protocol

B. Natural Language Processing

C. New Learning Platform

D. Non-Linear Programming

13. Cybersecurity is concerned with:

A. Designing websites

B. Protecting systems from digital attacks

C. Creating databases

D. Managing hardware

14. The digital divide refers to:

A. Differences between hardware and software

B. Unequal access to technology

C. The gap between AI and human intelligence

D. Differences between cloud and local storage

15. Which ethical framework focuses on rules and duties?

A. Utilitarianism

B. Virtue ethics

C. Deontological ethics

D. Relativism

16. Malware is:

A. A type of hardware

B. Malicious software designed to cause harm

C. A programming language

D. A cloud storage service

17. An expert system in AI is designed to:

A. Play video games

B. Replicate human expert decision-making

C. Store files in the cloud

D. Manage network traffic

18. Which is an example of application software?

A. Windows 11

B. A device driver

C. Microsoft Excel

D. BIOS

19. The right to be forgotten relates to:

A. Computer reliability

B. Information privacy

C. Intellectual property

D. Professional ethics

20. Responsible vulnerability disclosure is related to:

A. Privacy

B. Security ethics

C. Intellectual property

D. Work and wealth

Answers to True/False Questions

1. *False.* Hardware refers to the physical components of a computer system, not software programs.

2. *True.* An operating system manages hardware and provides a platform for applications.

3. *False.* AI is used across many industries including healthcare, finance, manufacturing, and education.

4. *True.* A requirements specification documents what the system must do and how it should perform.

5. *True.* Non-functional requirements describe system performance, usability, and reliability.

6. *False.* Wireframes show a simple structural layout, not the detailed final design.

7. *True.* Ethics is the branch of philosophy that examines right and wrong.

8. *False.* Morality refers to personal beliefs; ethics provides a more systematic framework.

9. *True.* GDPR provides individuals with rights over their personal data.

10. *False.* Intellectual property also applies to digital creations such as software and digital content.

11. *False.* Anonymity can have positive outcomes (e.g. whistleblowing) and negative outcomes.

12. *True.* Professional codes such as the BCS Code of Conduct guide ethical behaviour.

13. *True.* Software piracy is the unauthorised copying or distribution of copyrighted software.

14. *False.* Computer reliability is also an ethical concern because failures can harm people.

15. *True.* The digital divide describes unequal access to technology across populations.

16. *True.* Encryption converts data into a coded format to prevent unauthorised access.

17. *False.* Phishing is a fraudulent cyberattack, not a legitimate marketing method.

18. *False.* Cloud storage still carries security risks including data breaches and provider vulnerabilities.

19. *True.* AI systems can inherit and amplify biases present in their training data.

20. *False.* The BCS Code of Conduct applies to all IT professionals, not just developers.

Answers to Multiple Choice Questions

1. (C) Keyboard

2. (B) Operating systems

3. (C) SSD

4. (B) Machine learning

5. (B) A simple layout showing structure

6. (C) Gantt chart

7. (C) Outcomes and consequences

8. (B) General Data Protection Regulation

9. (C) Reproducibility

10. (C) The British Computer Society

11. (C) System response time under 2 seconds

12. (B) Natural Language Processing

13. (B) Protecting systems from digital attacks

14. (B) Unequal access to technology

15. (C) Deontological ethics

16. (B) Malicious software designed to cause harm

17. (B) Replicate human expert decision-making

18. (C) Microsoft Excel

19. (B) Information privacy

20. (B) Security ethics