Topic 5 Ethics and Laws

Key exam focus: Questions on this topic are typically **extended response** (6–12 marks) requiring you to: (1) identify relevant legislation or ethical principles, (2) apply them to a given scenario, (3) discuss multiple perspectives, (4) evaluate and reach a justified conclusion. Learn to balance different viewpoints and structure arguments clearly.

Key terminology

Term	Definition
Personal data	Any information relating to an identifiable living individual
Data controller	Organisation that determines how and why personal data is processed
Data processor	Organisation that processes data on behalf of a controller
Data subject	The individual whose personal data is being processed
Unauthorised access	Accessing computer systems or data without permission or beyond authorised scope
Intellectual property	Legal rights protecting creations of the mind (software, designs, inventions)
Copyright	Legal right giving creators control over use of their work
Fair dealing	Permitted exceptions to copyright for research, criticism, education
Piracy	Illegal copying or distribution of copyrighted material
Surveillance	Monitoring of behaviour, activities, or communications
Digital divide	Gap between those with and without access to digital technology
Algorithmic bias	Systematic unfairness in automated decision-making systems
Unicode	Universal character encoding standard supporting all writing systems
E-waste	Discarded electronic equipment, often containing hazardous materials

Must-know concepts

The four key acts

Four pieces of UK legislation regulate computing activities:

- **Data Protection Act 1998** — protects personal data
- **Computer Misuse Act 1990** — criminalises hacking and malware
- **Copyright Designs and Patents Act 1988** — protects intellectual property
- **Regulation of Investigatory Powers Act 2000** — governs surveillance

You must know the purpose, key provisions, and typical applications of each act.

Distinguishing moral, ethical, legal, and cultural

Legal — what the law requires or prohibits. Breaking the law has legal consequences (fines, imprisonment).

Ethical — principles of right and wrong conduct in a professional or social context. May go beyond legal requirements.

Moral — personal beliefs about right and wrong, often shaped by upbringing, religion, or philosophy.

Cultural — practices, values, and norms of a particular group or society. Varies across regions and communities.

Technology impacts to consider

Digital technology creates both **opportunities** and **risks**:

- **Workforce** — automation, remote working, job displacement
- **Privacy** — data collection, surveillance, personal information
- **Environment** — energy consumption, e-waste, paperless offices
- **AI** — automated decision-making, bias, accountability
- **Communication** — censorship, fake news, offensive content

Stakeholder perspectives

When analysing issues, consider different viewpoints:

- **Individuals** — privacy, convenience, employment
- **Organisations** — efficiency, costs, liability
- **Society** — equity, access, public good
- **Government** — security, regulation, enforcement

Good exam answers acknowledge multiple perspectives and potential conflicts between stakeholder interests.

Legislation quick reference

Act	Purpose	Key provisions	Typical violations
Data Protection Act 1998	Protect personal data of individuals	8 principles, data subject rights, registration	Selling customer data, poor security, keeping data too long
Computer Misuse Act 1990	Criminalise hacking and malware	3 levels of offence with increasing penalties	Hacking accounts, spreading viruses, DDoS attacks
Copyright Designs and Patents Act 1988	Protect intellectual property	Automatic protection, licensing, fair dealing	Pirating software, copying code, distributing films
RIPA 2000	Regulate surveillance powers	Interception warrants, directed surveillance, encryption keys	Unlawful surveillance, refusing to decrypt data

Data protection legislation

What is the data protection legislation?

Data protection legislation is a law that ensures **personal data is collected, stored, and used fairly, safely, and only for specific purposes**.

Data Protection Act — The 8 principles

1. Fair and lawful — Data must be processed fairly and lawfully, with valid legal basis
2. Purpose limitation — Data collected only for specified, explicit, and legitimate purposes
3. Data minimisation — Data must be adequate, relevant, and not excessive for the purpose
4. Accuracy — Data must be accurate and kept up to date where necessary
5. Storage limitation — Data kept no longer than necessary for the specified purpose
6. Security — Appropriate technical and organisational measures to protect data
7. Rights of individuals — Data subjects have rights to access, correct, and delete their data
8. International transfers — Data not transferred outside EEA without adequate protection

Computer Misuse Act — The 3 offences

Level	Offence	Example	Maximum penalty
Section 1	Unauthorised access to computer material	Guessing someone's password to read their emails	Up to 2 years imprisonment
Section 2	Unauthorised access with intent to commit further offence	Hacking into a bank system to commit fraud	Up to 5 years imprisonment
Section 3	Unauthorised modification of computer material	Spreading a virus, deleting files, DDoS attack	Up to 10 years imprisonment

Intellectual property protection

- Intellectual property (IP) refers to creations of the human intellect and how copyright, patents and trademarks protect IP.
- Licensing allows the creator of a software application to specify how it can be used and distributed.
- Difference between open-source and proprietary licences.
- Patent protects intellectual property

Protection type	What it protects	Example
Copyright	Creative works (text, music, images, software code)	A song, a photograph, a computer program
Patent	Inventions and new processes	A new type of processor, a hardware invention
Trademark	Brand names, logos, slogans	Company logo, product name, advertising slogan
Licensing	Grants permission to use protected work under specific terms	Software licence, music streaming rights

Patents A patent prevents someone copying/using/selling an invention because it gives the inventor the exclusive right to reproduce/use/sell it for 20 years. A person/organisation that infringes a patent can be prosecuted, because it gives the inventors the legal protection to defend their exclusive right

The **Copyright, Designs and Patents Act 1988** protects the intellectual property of creators, giving them exclusive rights to their work. In computing, this primarily applies to software, databases, and digital content.

What copyright protects

- **Software** — source code, compiled programs, and algorithms expressed in code
- **Databases** — the structure and arrangement of data (not the facts themselves)
- **Digital content** — music, films, images, ebooks, websites
- **Documentation** — user manuals, specifications, design documents

Key features

- **Automatic protection** — copyright exists automatically when a work is created; no registration required
- **Duration** — typically lasts 70 years after the creator's death
- **Exclusive rights** — only the copyright holder can copy, distribute, rent, or adapt the work
- **Licensing** — copyright holders can grant others permission to use their work under specific terms

Infringement examples

- Downloading pirated software, music, or films
- Copying and distributing software without a licence
- Using copyrighted images on a website without permission
- Copying code from open-source projects without following licence terms
- Sharing ebooks or academic papers without authorisation

Fair dealing exceptions

Limited use of copyrighted material is permitted for:

- Research and private study (non-commercial)
- Criticism, review, and news reporting
- Education (limited copies for classroom use)

Data Privacy and Protection:

The obligation to manage personal data securely, ensuring it is accurate, relevant, and not kept longer than necessary.

Examples of how personal data can be collected include:

- GPS
- Number plate/face recognition
- Smart listening devices
- Signing up to services, organisations and products
- Customer surveys
- Electronic tagging
- Official purposes - council/government/medical services

The collection of personal data raises many ethical and legal issues such as:

- Privacy
- Data protection
- Misuse
- Cookies

Give two pieces of information that organisations must tell people when requesting consent to use their personal data.

- That they are giving consent for the organisation to store data
- What the data is being collected for
- What processing will be done on their data
- That they can withdraw consent at any time
- How long it will be stored

That the data will be stored securely

Examples of privacy issues in computing

Face recognition

The increase in cameras and advances in technology means face recognition is possible, whilst this can mean an advantage in crime prevention/detection, people are concerned about privacy. Privacy concerns include, what else is being watched? and who is watching?

GPS

GPS is built-in to most smart phones and brings with it a number of features that many see as a benefit, 'find my phone 'for when it gets lost/stolen, location tagging in photos and for navigation software. Some users are concerned with where this data is kept? , who might have access to it? and is it being used for any other purposes?

Internet monitoring

Most schools and businesses use monitoring software to track their students' and employees' internet activity

Social media companies also employ similar tools to detect and remove illegal or harmful content like hate speech, misinformation, or violent threats Arguments for, these measures promote responsible online behaviour and prevent Cyberbullying Arguments against, concerns about limitations to free speech, potential abuse by authorities who control the monitoring systems, and biased algorithms leading to censorship

Regulation of Investigatory Powers Act 2000 (RIPA)

The Regulation of Investigatory Powers Act 2000 regulates the powers of public bodies to conduct surveillance and investigate communications. It attempts to balance national security needs with individual privacy rights.

Key powers regulated

- Interception of communications — monitoring phone calls, emails, and internet traffic
- Acquisition of communications data — obtaining metadata (who contacted whom, when, from where)
- Directed surveillance — covert observation of specific individuals
- Intrusive surveillance — surveillance in private vehicles or residences
- Use of covert human intelligence sources — informants and undercover officers
- Encryption and RIPA
- RIPA gives authorities the power to demand that individuals hand over encryption keys or decrypt data. Refusing a lawful demand to provide encryption keys is a criminal offence, punishable by up to 2 years imprisonment (or 5 years in cases involving national security or child indecency).

Controversy and debate

RIPA has been controversial due to concerns about:

- Scope of surveillance powers being too broad
- Local authorities using powers for trivial matters
- Potential for abuse without adequate oversight
- Balance between security and privacy

AI and Robotics:	**Environmental Impact:**	**Censorship and the Internet**

Ethical concerns involving accountability, safety, bias in algorithms, and legal liability when autonomous systems fail.

Issue	Description	Example
Accountability	Who is responsible when AI makes a mistake?	Self-driving car causes an accident — who is liable?
Bias	AI systems may reflect biases in training data	Facial recognition less accurate for certain demographics
Safety	Ensuring AI systems operate safely	Medical diagnosis AI must be reliable
Job displacement	Automation replacing human workers	Robots in factories, automated customer service
Privacy	AI systems processing personal data	Facial recognition in public spaces

Causes of algorithmic bias

- Machine learning having been trained using insufficient/inappropriate data
- Human bias leading to discrimination and a lack of fairness
- Poor design of the algorithm

Methods available to reduce the risk of algorithmic bias

- Human oversight and 'sense checking' and confidence/error ratings of predictions
- Governance (anticipating and managing risks and make sure legal requirements are adhered to)
- Improve the training data

The energy consumption of data centers, the lifespan of devices, and the disposal of electronic waste (e-waste).

Stage	Environmental issue	Key exam phrases
Manufacture	Extraction of raw materials, energy used in production	"Extraction of metals", "fossil fuels used", "water consumption"
Use	Energy consumption during operation	"Electricity consumption", "carbon footprint", "data centres"
Disposal	E-waste, toxic materials, landfill	"E-waste", "hazardous materials", "landfill", "pollution"
Replacement cycle	Frequent upgrades increase all of the above	"Shorter replacement cycles", "more manufacturing", "more disposal"

Actions:

- Use it as long as possible/don't replace it
- Sell/give it to a company that will recondition it
- Give it away to a friend or charity
- Repair it if it breaks
- • Keep the software updated

The Internet raises complex questions about free speech, harmful content, and the role of governments and platforms in controlling information.

Arguments for some Internet regulation

- Protecting children from inappropriate content
- Preventing incitement to violence and terrorism
- Combating illegal activities (child exploitation, drug dealing)
- Controlling dangerous misinformation (health, elections)
- Protecting national security

Arguments against censorship

- Free speech is a fundamental human right
- Censorship can be used to suppress legitimate political dissent
- Difficult to define what should be censored
- Technical measures can be circumvented
- Censorship often affects marginalised groups disproportionately

Who should decide?

- **Governments** — elected but may abuse power; laws vary by country
- **Platforms** — technical capability but unaccountable private companies
- **Users** — individual choice but may not protect vulnerable people
- **Courts** — due process but slow and expensive

Data breach scenario

Question: A hospital suffers a cyber attack where patient records including names, addresses, medical histories, and treatment plans are stolen. The attackers threaten to publish the data unless a ransom is paid.

(a) Identify which legislation is relevant to this scenario. [2 marks]

(b) Explain the hospital's obligations under the Data Protection Act following this breach. [4 marks]

(c) Discuss the ethical considerations the hospital faces in deciding whether to pay the ransom. [6 marks]

(a) Relevant legislation:

Data Protection Act 1998/2018 — the hospital is a data controller responsible for protecting patient data [1 mark]. Computer Misuse Act 1990 — the attackers have committed offences under Sections 1, 2, and 3 [1 mark].

(b) DPA obligations:

The hospital must report the breach to the Information Commissioner's Office (ICO) within 72 hours if it poses a risk to individuals' rights [1 mark]. It must notify affected patients if there is a high risk to their rights and freedoms [1 mark]. It must document the breach, its effects, and remedial actions taken [1 mark]. The hospital may face fines if found to have inadequate security measures (breach of Principle 6) [1 mark].

(c) Ethical considerations:

Arguments against paying:

Paying encourages further attacks on this and other organisations. There's no guarantee attackers will delete the data or not publish anyway. The money may fund criminal or terrorist activities [2 marks].

Arguments for paying:

Publication could cause severe harm to vulnerable patients (mental health records, HIV status). The hospital has a duty of care to minimise harm to patients. If the alternative is certain publication, payment might reduce harm [2 marks].

Conclusion:

Most ethical frameworks and government guidance advise against paying ransoms. The focus should be on supporting affected patients, improving security, and cooperating with law enforcement [2 marks].

Facial recognition in schools

Question: A school proposes implementing facial recognition technology to monitor student attendance and improve site security. Students would have their faces scanned when entering the building.

Evaluate this proposal, considering legal, ethical, and practical issues. [12 marks]

Level of Response

Level 3 response (9-12 marks):

Legal considerations:

Facial recognition data is biometric data, classified as sensitive personal data under the Data Protection Act. Processing requires explicit consent or another lawful basis. For children, parental consent would typically be needed. The school must demonstrate the processing is necessary and proportionate — less intrusive methods should be considered first [3 marks].

Ethical considerations — benefits:

Accurate attendance records could identify safeguarding concerns (children not attending). Security benefits could protect students from unauthorised visitors. Efficient registration could save time for teaching. Modern students are already familiar with biometric technology [3 marks].

Ethical considerations — concerns:

Normalising surveillance of children from a young age raises concerns about privacy expectations. Facial recognition systems have documented higher error rates for certain ethnic groups, potentially causing discrimination. Students should be able to make mistakes without permanent digital records. The power imbalance means consent may not be truly free [3 marks].

Practical considerations:

Systems may not work reliably in all conditions (lighting, crowds). Students may find ways to defeat the system. The technology requires significant investment and maintenance. Data breach could expose highly sensitive biometric data [2 marks].

Conclusion:

The potential benefits do not appear to justify the privacy intrusion, especially for children who cannot fully consent. Less invasive alternatives (card-based systems, traditional registration) can achieve similar goals without collecting biometric data. If implemented, strict safeguards, independent oversight, and clear data retention limits would be essential [1 mark].

Social media content moderation

Question: Social media platforms use a combination of AI and human moderators to remove content that violates their policies. Discuss the ethical challenges of content moderation. [6 marks]

Challenges of AI moderation:

AI struggles with context — satire, quotes, and counter-speech may be incorrectly flagged. Different languages and cultural contexts are harder for AI to understand. AI may have biases from training data [2 marks].

Challenges of human moderation:

Moderators must view traumatic content causing psychological harm. Scale makes it impossible to review all content. Human moderators also have biases and make inconsistent decisions [2 marks].

Broader ethical issues:

Platforms have immense power over public discourse without democratic accountability. Policies may be influenced by commercial rather than ethical considerations. Global platforms must navigate different cultural norms and legal requirements [2 marks].

Copyright considerations

Question: A student finds useful code on GitHub to help with their programming project. Discuss the copyright considerations they should be aware of before using this code. [4 marks]

Check the licence:

Code on GitHub is protected by copyright. The student must check the repository's licence (e.g., MIT, GPL, Apache) to understand what they're permitted to do with the code [1 mark].

Understand licence requirements:

Different licences have different requirements — some require attribution, some require derivative works to use the same licence (copyleft), some restrict commercial use [1 mark].

Attribution:

Most open-source licences require the original author to be credited. The student should include appropriate attribution in their project [1 mark].

No licence = full copyright:

If there's no explicit licence, the code is under full copyright protection and technically cannot be used without the author's permission [1 mark].

Computer Misuse Act application

Question: A disgruntled employee who has been given notice uses their still-active login credentials to access the company network, download client contact lists, and then delete important project files before leaving. Which sections of the Computer Misuse Act apply? [6 marks]

Section 1 — Unauthorised access:
Although the employee has valid login credentials, accessing the network to download data for personal use (taking to a competitor) exceeds their authorisation. Access for purposes outside their job role is unauthorised [2 marks].

Section 2 — Intent to commit further offence:
Downloading client contact lists with intent to take them to a competitor could constitute theft of trade secrets or breach of confidence — a further offence [2 marks].

Section 3 — Unauthorised modification:
Deliberately deleting project files is unauthorised modification of computer material, causing damage to the company's data and potentially its business operations [2 marks].

Digital divide and access equity
The digital divide refers to the gap between those who have access to digital technology and those who don't. This creates significant social and economic inequalities.

Question: A local council is moving all its services online to reduce costs. Discuss the ethical implications of this decision for different groups in the community. [8 marks] Level of Response
Impact on elderly residents:

Many elderly people may lack digital skills, internet access, or confidence to use online services. They may be unable to access essential services they previously used easily. This could lead to social exclusion and difficulty accessing benefits or support they're entitled to [2 marks].

Impact on low-income residents:
Those who cannot afford broadband or devices may be excluded. Using library computers or mobile data may be impractical for completing complex forms. The cost savings benefit the council, but costs shift to vulnerable residents [2 marks].

Impact on disabled residents:
Online services may not be fully accessible to people with visual impairments, motor disabilities, or cognitive difficulties. Poorly designed services could create new barriers [1 mark].

Potential benefits:
Online services can be available 24/7, which benefits working people. Well-designed services could be more accessible for some disabled users. Cost savings could be redirected to other services [1 mark].

Mitigation measures:
The council should maintain some face-to-face or phone services for those who cannot use online systems. Digital skills training and assisted access at libraries could help. Services must meet accessibility standards [2 marks].

Cultural considerations

Technology exists within cultural contexts that affect how it is designed, used, and experienced by different groups. Cultural considerations are important for creating inclusive technology and understanding global digital issues.

Layout considerations

Design conventions vary by culture and can affect usability:

- Reading direction — Western languages read left-to-right; Arabic and Hebrew read right-to-left; some Asian languages read top-to-bottom
- Menu and navigation placement — should align with reading direction expectations
- Form layouts — address formats, name order (family name first vs last), date formats vary globally
- Information density — some cultures prefer more content per page, others prefer minimalism

Colour paradigms

Colour meaning variations

Colours carry different meanings in different cultures.

Colour	Western meaning	Other cultural meanings
Red	Danger, stop, error, passion	China: luck, prosperity, celebration. India: purity, fertility
White	Purity, cleanliness, peace	Many Asian cultures: death, mourning, funerals
Green	Nature, go, success, environment	Islam: sacred colour. Ireland: national identity
Yellow	Caution, happiness, warmth	Japan: courage. Egypt: mourning
Blue	Trust, calm, professional	Relatively consistent globally, often seen as safe choice

Character encoding

Different writing systems require different character encoding support:

ASCII — 7-bit encoding supporting 128 characters (basic Latin alphabet)

Extended ASCII — 8-bit supporting 256 characters (includes accented European characters)

Unicode (UTF-8, UTF-16) — supports over 143,000 characters from virtually all writing systems

Question: A UK company is developing an e-commerce website that will be used by customers in Japan. Describe three technical considerations related to cultural differences that the developers should address. [6 marks]

Character encoding:

The website must support Japanese characters (hiragana, katakana, kanji). Unicode (UTF-8) should be used throughout the system, including the database, to correctly store and display Japanese text [2 marks].

Input methods:

Japanese users type using romanised input that converts to Japanese characters. Form fields must support input method editors (IME) and not interfere with the conversion process [2 marks].

Date and address formats:

Japan uses year-month-day date format and addresses are written from largest to smallest unit (prefecture, city, district, building). Forms and displays must accommodate these conventions [2 marks].

Accessibility requirements

Question: A small business is developing a new website. The owner believes that making the site fully accessible to users with visual impairments would be too expensive for a small company.

(a) Explain two ways websites can be made more accessible to visually impaired users. [4 marks]

(b) Discuss the legal and ethical arguments for requiring accessibility. [6 marks]

(a) Accessibility measures:

Alt text for images: All images should have descriptive alternative text that screen readers can read aloud, allowing visually impaired users to understand the content and purpose of images [2 marks].

Keyboard navigation: All functionality should be accessible using keyboard only, without requiring a mouse, as many visually impaired users navigate with screen readers and keyboards [2 marks].

(b) Legal and ethical arguments:

Legal: The Equality Act 2010 requires service providers to make reasonable adjustments for disabled people. Websites are considered a service, and inaccessibility could constitute discrimination. Public sector websites must meet specific accessibility standards by law [3 marks].

Ethical: Excluding disabled users from online services denies them equal participation in society. As more services move online, inaccessible websites create significant practical barriers. The additional cost of building accessibility in from the start is typically small. Ethical businesses should aim to serve all potential customers [3 marks].

Open source vs proprietary software

Feature	Open Source Software	Proprietary Software

Definition	Software where the **source code is publicly available**	Software where the **source code is kept private**
Who controls it	Community of developers or an organisation	A single company or organisation
Cost	Usually **free**, but support may cost money	Usually **paid** (one-off purchase or subscription)
Source code access	Users can **view, modify, and share** the code	Users **cannot access or modify** the code
Customisation	Highly customisable	Little or no customisation
Security	Bugs may be found quickly due to many developers reviewing code	Security fixes depend on the company
Support	Community forums or paid third-party support	Official customer support provided
Updates	Frequent, community-driven	Released on the company's schedule
Examples	Linux, LibreOffice, Firefox	Windows, Microsoft Office, Adobe Photoshop
Typical users	Developers, schools, organisations wanting flexibility	Businesses and individuals wanting ease of use

Question: A charity is deciding whether to use open-source or proprietary software for its operations. Discuss the ethical considerations involved in this choice. [6 marks]

Arguments for open source:

Open-source software is typically free, allowing the charity to direct more funds to its mission. The transparency of open source means the charity can verify what the software does with their data. Open source supports digital commons and knowledge sharing, aligning with charitable values [2 marks].

Arguments for proprietary:

Proprietary software often comes with professional support, reducing risk for organisations without technical expertise. Commercial software companies have accountability and resources if things go wrong. Some proprietary software offers charity discounts, making cost differences smaller [2 marks].

Broader considerations:

The charity should consider what skills are available to support the chosen solution. Vendor lock-in with proprietary software could create future problems. The charity's donors and stakeholders may have views about responsible use of funds. Data protection obligations apply regardless of software choice [2 marks].