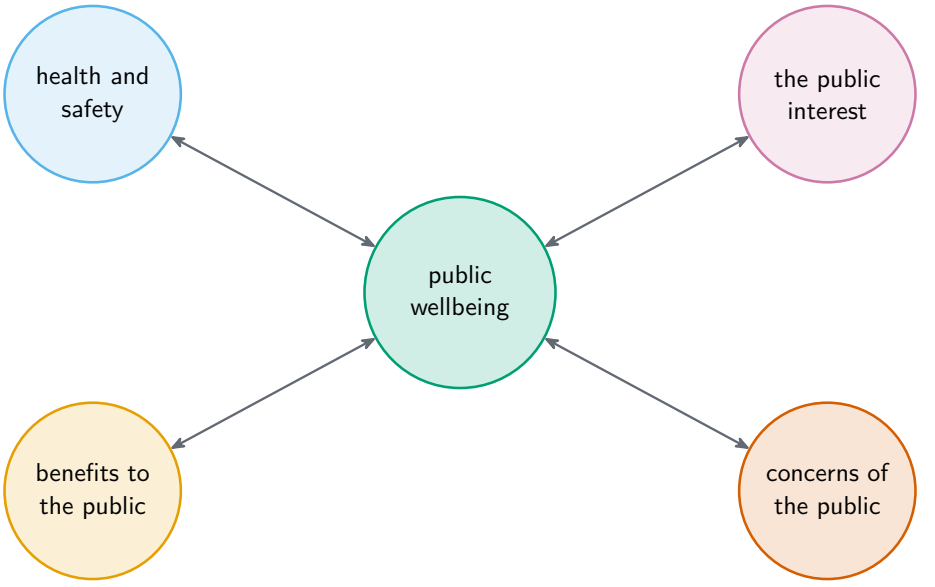
Impact of Computing

AP Computer Science Principles

Beneficial and Harmful Effects

A pile of e-waste – computing has environmental costs as well as benefits

Every computing innovation can be used in ways that **help** and ways that **harm** – often the same technology does both. A social network connects people **and** can spread misinformation; automation raises productivity **and** can remove jobs. Effects are frequently **unintended**: creators cannot foresee every use. When you evaluate a computing innovation, weigh its benefits and harms on people and society, and remember that harms are not always deliberate.

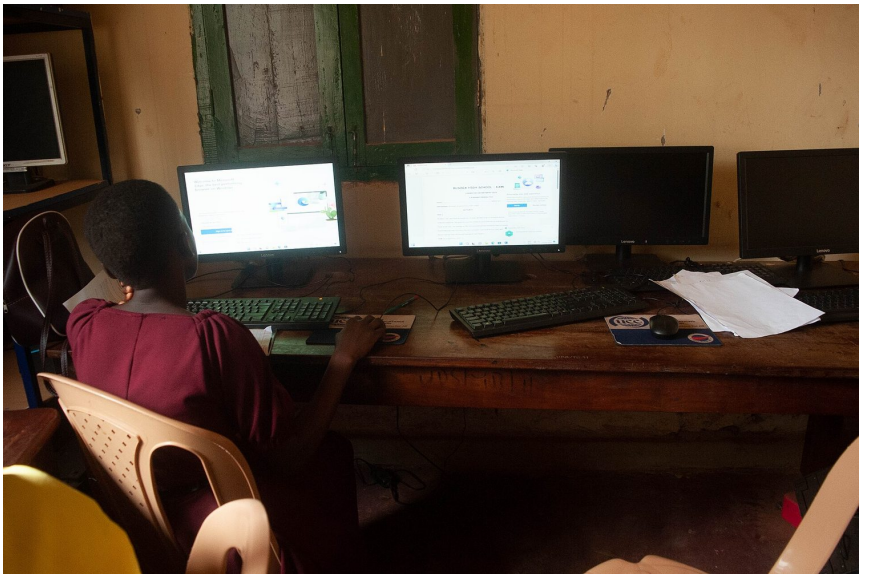


Computing affects the public's wellbeing in several ways

Computing also generates creativity in other fields, which the CED asks for as a benefit in its own right, not merely as convenience: modelling and imaging in **medicine**, simulation in **engineering**, new forms in the **arts** and music, and new kinds of **communication** entirely. An innovation's beneficial effects are often in a field far from computing.

The Digital Divide

The **digital divide** is the unequal access to computing and the Internet across groups – by income, geography, age, or country. Those with access gain education, jobs, and services; those without fall further behind. The divide is shaped by economic, social, and geographic factors, and efforts to close it (affordable devices, public access, infrastructure) aim to make computing's benefits fairer.



Public library computers: digital divide is about unequal access to devices, connectivity and skills

A rural satellite dish: geography still shapes who gets fast internet and who waits

Computing Bias

A self-driving car on a city street – autonomous systems raise safety and bias questions

Bias can be built into computing systems – often unintentionally. If the **data** used to build a system reflects existing prejudice, or if the designers' assumptions are one-sided, the system can produce **unfair** results (for example, a hiring tool that favors one group). Bias can enter at every stage – data collection, design, and use – so systems should be tested for fairness across different groups. Recognizing that "the computer said so" is not the same as "fair" is an important habit.

Crowdsourcing

Crowdsourcing obtains input, ideas, or funding from a **large group of people**, usually online. It harnesses the knowledge and effort of many – mapping projects, product reviews, citizen science, and **crowdfunding** all rely on it. The Internet makes crowdsourcing possible at a scale and speed never before achievable, letting a project draw on contributors worldwide.

A Wikipedia edit-a-thon: crowdsourcing pools many people's work into a shared resource

Legal and Ethical Concerns

A CCTV control room: surveillance systems trade safety gains against privacy concerns

Computing raises questions of law and ethics:

- **Intellectual property** and **copyright** protect creators' work; using it may require permission or a license. **Open-source** and **Creative Commons** licenses let creators share work under stated terms.
- **Plagiarism** – using others' work as your own – is unethical and often illegal.
- Collecting and using personal data raises **privacy** questions about consent and misuse.

The three "open" terms, which are not the same thing

Term	What it means
open source	programs that are **made freely available and may be redistributed and modified** by anyone. The licence grants those rights explicitly – free of charge is not the same as open source, and a free program you may not modify is not open source.
open access	research and other content made available online **without charge**, so a reader does not need a subscription. It says nothing about the right to modify.
Creative Commons	a family of licences a creator applies to their own work to grant specific permissions in advance – for example "you may reuse this if you credit me" or "you may reuse this but not commercially".

All three are ways of **granting** rights the creator holds by default under copyright. That is why they matter for the exam: copyright is automatic, so anything not explicitly licensed is restricted, and using it needs permission.

Just because something is technically possible does not make it legal or ethical.

What is recorded while you browse

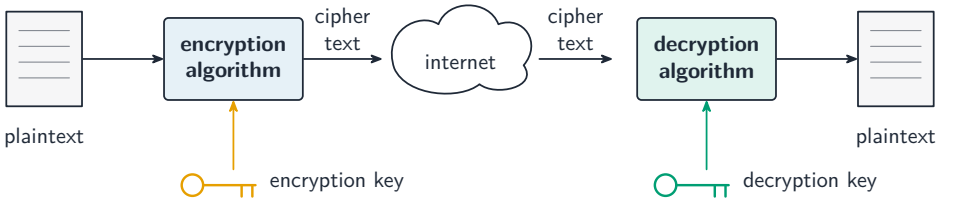
Two collection routes the CED names, and neither needs you to type anything:

- **Websites can record and maintain a history of the individuals who have viewed their pages** – which pages, when, how long, and from which device.
- **Search engines can use your search history** to suggest websites, and to sell **targeted marketing**: the advertisement follows the search, which is why a product looked up once then appears for weeks.

Neither is inherently malicious, and both are the mechanism behind services people find useful. The point the exam wants is that **data collected for one purpose can be combined and used for another**, often without the person realising they agreed to it.

Safe Computing

Protecting personal data is a shared responsibility. Key ideas:



Encryption scrambles plaintext with a key; only the key can decrypt it

- **Personally identifiable information (PII)** (name, address, ID numbers) should be shared carefully, because it can be misused for **identity theft** .
- Threats include **phishing** (tricking you into revealing information), **malware** , and weak passwords.
- **A malicious link can be disguised** on a web page or in an email message: the text you see and the address it actually goes to are separate, so a link reading `www.yourbank.com` can point anywhere. Hover to see the real destination before clicking, and be most suspicious of a link that arrives unexpectedly and creates urgency.
- Defenses include strong, unique **passwords**, **multi-factor authentication** , **encryption** (scrambling data so only authorized people can read it), and keeping software updated.

Encryption is the central tool for keeping data private in transit and storage. Being a responsible computer user means protecting your own and others' information.

Exam skill: be able to identify the beneficial and harmful effects of a given innovation, explain a privacy or security risk, and name a safe-computing practice that addresses it.

> **Worked example.** A hiring algorithm is trained on a company's past hires, who were mostly one group, and it then rejects qualified applicants from other groups. Name the problem and its cause: this is **computing bias**, caused by biased training data – the model learned the historical pattern instead of a fair rule. A full-mark exam answer states the harm (qualified people are unfairly rejected) **and** its cause (the bias came from the data, not the code).

Exam tips

- Argue **both** the beneficial and harmful effects of a computing innovation – a balanced answer scores best.
- Use correct terms for data concerns: **PII**, privacy, security, and **algorithmic bias**.
- Explain how **crowdsourcing** and large data sets create value and raise new risks.
- Distinguish the **digital divide** (access) from bias (fairness) and give a concrete example of each.
- Tie every claim to a specific innovation and effect, as the written response demands.