Ethical topics

1. Introduction

We have many laws which govern the use of computer systems and the handling of data. Most of us are aware if our actions are illegal and the majority of us would never consider doing anything that could potentially end up with a huge fine or even a jail sentence.

When we think about the use of technology, we also need to be aware of the moral and ethical issues. Just because something is legal, it doesn't necessarily mean that it is acceptable or right.

Much of the technology we use is still so new that boundaries are inevitably pushed and even when organisations try their best, there is the risk of of something happening which, in hindsight, is later considered as unethical.

So what are ethics and why do they matter?

Ethics consists of the standards of behaviour that are acceptable within our society. They are the moral principles and values that make society operate effectively and justly.

Unethical behaviour undermines trust and can lead to a loss of respect and goodwill. People often feel anger and hostility towards a person/organisation that has operated unethically.

We have covered a range of topics that touch upon ethical issues and technology. However, this is such a vast subject that in your exam you could be asked about many different scenarios. When answering a question, always try to think about the moral viewpoints and how they affect different stakeholders. You will be expected to discuss both sides of any issue and then conclude with your own opinion.

Ethical topics

2. The internet and social media

The internet is an amazing resource. We use it on a daily basis for entertainment, socialising, research, shopping and so many more things. Always available, 24 hours a day, 7 days a week, 52 weeks of the year. It's hard to imagine a life without it.

Most of us use social media sites to keep in touch with family and friends. Facebook, Instagram, Snap Chat, Twitter and many others. People would probably say that their experiences of these sites are positive.

No one owns the internet. No one manages it. No one is responsible for it. This is both the greatest benefit and greatest drawback of the Internet.

The lack of a centralised authority makes it easy for people to be anonymous and bully or troll others. Upsetting, gruesome and inappropriate images are regularly shared and it can be quite a shock to see an unasked-for image appear in your news feed.

These sites are owned and operated by organisations.

We don't pay a fee to use them, but the owners make money from advertising and sponsorship.

Do they have an ethical and moral obligation to make sure that all content posted on their platform is acceptable? Should they be held accountable for obscene or inappropriate content that their users put online?

They do make tremendous efforts to keep the worst of it off their platforms but there are always grey areas where it is one person's opinion versus another person.

Ethical topics

3. The internet, social media and stakeholders

If you are asked a question about this topic in the exam, you need to discuss the potential issues and consider how they affect each of the different groups of stakeholders.

So who are the stakeholders?

You, and all of the other **users of these sites** are stakeholders. How would the issues highlighted on the previous page affect you? How might they affect younger/older people or those who are vulnerable?

The **organisation who owns the service** is another stakeholder. What are their responsibilities? Who should they be protecting? What might happen to them if they continue to allow unethical content on their platforms? How might the public perceive them if they continue to read news stories about them? How might they be affected if advertisers decided they didn't want to be associated with the platform any longer?

Businesses / individuals who pay to advertise are another stakeholder. How might they be affected by negative news stories? Would it reflect badly on their own business?

Ethical topics

4. Digital Divide

There are people in this country who cannot afford to buy and run a computer. This means that they, and their family, begin to fall behind others who regularly use computers.

When they want to apply for a job they might find it harder to compete with others who are familiar with computers and software applications. Their children could be disadvantaged because a lot of homework and projects now require research using the Internet.

The digital divide is also apparent between countries. A lot of people in the UK, Europe and the U.S. are confident users of technology. Whereas people who live in rural parts of say Africa might never have seen a computer. Even if they could afford to buy one, they might not have the electricity to run one or the training in how to use the applications.

Factors that cause a divide are

- Money - access is not free
- Language - a large part of the Internet is written in English
- Literacy - most of the internet includes text
- Age - older generations generally find new technology harder to use
- Physical - many people have disabilities that make using the internet more difficult than it should be.

Ethical topics

5. Ethics and the digital divide

There is no question that the digital divide exists, but is it an ethical issue? Do you think that everyone in this country should have the same rights and access to technology? How about between countries i.e. should people in third world countries have the same opportunities that we have?

Who are the stakeholders?

The government**: In order for our economy to grow we need skilled, employed workers. Is the government** responsible for ensuring that there are sufficient training schemes in place? Where does the money come from to provide these?

Is it fair to assign a large budget to giving away free or discounted computers while health and education systems are struggling to make ends meet? Or will making sure that society is fully computerised and connected end up paying for itself as people become more productive and happy?

Organisations - businesses want skilled workers. Should they take responsibility and help provide training? Or can they expect the government to do this for them?

Individuals - is it up to everyone to ensure that they learn the skills they need? Should they pay for it themselves or do they have the right to expect training opportunities to be provided for them?

What about **overseas countries**? Should their own governments be responsible for funding training and equipment or should richer countries be providing more help and assistance to enable them to catch up and compete on a level playing field?

Ethical topics

6. Whistleblowing

Governments and private companies do not always do the right thing. And sometimes they do the wrong thing, but keep it secret. When a worker discovers something is going on that they disagree with, they have to consider

whether they are willing to risk their jobs or their freedom to let others know about the issue.

The people leaking this information are usually breaking the law to do it, because they believe that the public should know about it. But once it is made public, information can't be taken back.

The Internet is a powerful tool for spreading information. Organisations such as WikiLeaks and Cryptome will accept and publish information from whistleblowers.

In the past, whistleblowers have accidentally released harmful data alongside what they were trying to protest - the identities of active military or intelligence personnel, for example.

Diplomatic information released through WikiLeaks is believed to have been one of the major causes of the Arab Spring - the series of political revolutions that sprang up across the Middle East throughout the 2010s. People have died because of the leaks, but they inspired others to protest against unfair and unjust governments.

Do the public have a right to *all* information that their governments have, or are there things that should be kept secret? Do individual workers have the right to make that decision? And can we trust organisations like WikiLeaks to publish what they receive in a safe and unbiased manner?

This is where the controversy lies.

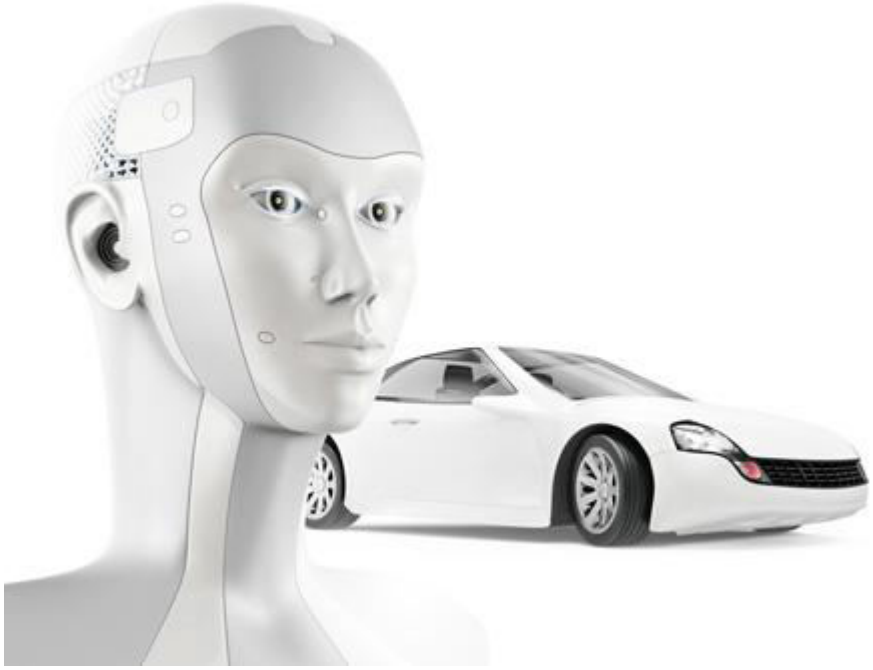
Ethical topics

7. Self-driving vehicles

If your car was about to hit a child crossing the street, would you swerve out of the way if it meant hitting two adults on the other side of the road?

Cars kill around 2,000 people in the UK every year, and tens of thousands more across the world. Computer scientists are hard at work making cars safer, and one of the ways this might be done is by taking humans out of the driver seat - having cars drive themselves. The ethical decisions a self-driving car has to make are no different from those a human driver will face. But it is up to their programmers to work out what their responses will be.

How should the car be programmed to act when an accident is unavoidable? Should they prioritise the driver? Other drivers? Pedestrians?



Another ethical question that self-driving vehicle technology forces us to face is this: How much safer does a self-driving car have to be before it is no longer ethical to allow humans to drive at all?

As mentioned above, human drivers kill 2,000 UK citizens every year. If completely switching to self-driving cars would lower that number to just 1,990, is it ethical to force people to give up their cars and buy new ones with self-driving technology? How about if it could drop fatalities to just 1,000, or 100, or 0?

What might happen if hackers found a way to access and control self-driven cars?

Self-driving vehicles are already starting to appear on roads, and they will become increasingly common sights as time goes by. It is up to us to decide how to use this technology.

Ethical topics

8. Genetic screening

It is now practical and possible to get a comprehensive genetic analysis of yourself. This is possible with sophisticated computerised DNA sequencing machines.

You supply a DNA sample to a genetic analysis company and they provide a personalised report that includes insights into your ancestry, your genetic traits and health risks.

This information may be invaluable for someone who suspects they have inherited a family trait making them more likely to get a certain illness and so on. It could be invaluable for couples wanting to make family planning decisions.

Ethically this is not an issue in itself as it is you who wants to know - it is your genes after all

However, what if another organisation insists on also seeing that information? For example, a life insurance company wants to use it to assess risk. What if an employer wants to know? Clearly this becomes an ethical issue once that deeply private information becomes public information.

As you know, the rest of your relatives may also have the same genetic traits - what if they are stigmatised because of this information? Now, it not only affects you, it can affect other people as well through no fault of their own.

Furthermore, it is not too difficult to get a DNA sample of a person without their knowledge - a hair from a brush would be enough. Obtaining such a sample without their pesmission becomes an ethical issue.

We are just getting to the point where society has to decide how to handle this kind of data. Think about these issues:

- prenatal screening for potential issues or gender selection
- paternity tests without permission
- personal genetic traits and any likely risks.

Ethical topics

9. Drone warfare

While self-driving cars are programmed to prevent deaths, there are other machines that are programmed to cause them.

Drone warfare has become an increasingly important part of modern military doctrine. Unmanned robots patrol the skies above conflict zones. Some of them merely collect information and transmit it back to be analysed. But others can launch missiles at the push of a button...or with no input at all.

The argument in favour of drone warfare is that no soldiers have to risk their lives, and that their targetting systems can be more precise than a rifleman on the ground. But drones are increasingly controversial for how easy they make it to kill from afar, allowing for indiscriminate attacks. If more attacks are made, even if they are more precise, it results in higher collateral damage, anger and retribution among the surviving community of the attack.

It is also entirely possible to program drones to act completely independently of human drivers, to allow them to make targetting decisions based on their programming and the standing orders they received when they were launched.

Would taking humans out of the loop completely be ethical?

Environmental topics

1. Introduction

The environment and our need for ever-more energy has become two of the leading issues we have to face in our modern world.

This includes the use of fossil fuels, climate change, water management, deforestation and so on.

Computer technology has a key part to play.

It can help us to more efficiently extract the resources we need right now and it can help to handle the more harmful long term effects. On the other hand it also brings its own problems such as e-waste and increasing our energy needs.

In this section we discuss how technology is having an impact

Environmental topics


courtesy of Wikimedia Commons

2. E-waste

Electronic waste or e-waste is a huge problem around the world. Our old technology is often sent to landfill, not because it doesn't work, but simply because it has been replaced by a whizzy, all singing, all dancing, newer version.

The major problem with e-waste is that the toxic chemicals such as lead, arsenic and cadmium can leach into the soil over time. Then as rain washes it away, rivers and water supplies can be contaminated.

As a result most countries in the developed world have introduced strict regulations to prevent e-waste being dumped into landfill. Electronic components now have to be recycled.

In order to get around this, some countries have been sending their e-waste to less economically developed regions around the world where the regulations aren't as strict.

We hear of e-waste mountains where people (even children) spend their days in hazardous conditions salvaging some of the precious metals from the discarded electronic goods to sell for cash. This practice can have a huge detrimental effect on their health and safety.

Environmental topics

3. Sustainability

What must not be forgotten when you look at the mobile phone in your hand is that every single part of that phone, at some point, had to come out of the ground.

The plastic, the glass, the precious metals, rare minerals, steel, copper and all the other material that make up your phone, at some point had to be dug up as raw material. This raw material was then processed, refined, transported and shaped into each component.

So it does not make much sense to throw away all that material, energy and effort into landfill, never to be seen again.

A better way is to re-use as much of it as possible. The word is '**sustainability**' - making as much use of our existing resources as possible.

There are three main ways to do this, often referred to as the "Three Rs"

1. **R**educe
2. **R**euse
3. **R**ecycle

Environmental topics

4. Reduce, Reuse, Recycle

Reduce

Reducing the amount of waste produced is fairly easy to do personally - just buy less stuff, and throw less away! Don't replace devices that still work just because a new version has come out.

courtesy of Wikimedia Commons

Computer systems can help reduce the amount of waste produced by making manufacturing more efficient. When less material and energy is used to produce an item, throwing it away will have less impact on the environment.

Re-use

Just because you are done with your mobile phone or computer doesn't mean that nobody else has a use for it. It's easier than ever to find someone willing to buy second-hand computer peripherals and devices using the internet, giving devices a new lease of life with a new owner.

There are a number of schemes that will re-distribute the items you donate for other people to use. Some are commercial companies and others are charities.

Recycle

Although re-use is the best idea as the device remains intact, eventually a device breaks and can't be fixed. When this happens, the environmental impact of throwing away the remains can be minimised by salvaging as many of the components as possible, and breaking down the rest into their base materials. Those materials can then be recycled into new products.

Environmental topics

5. Energy use

Another effect of computer systems on the environment is the sheer amount of electricity used to power up the billions of computers around the world.

The rise of social networking and handheld computers such as tablets and mobile phones has led to a much higher daily use of electricity by the average person.

Electricity tends to produce greenhouse gases because of the way it is generated. Technology is helping to reduce greenhouse gas emissions by allowing for more environmentally-friendly sources such as wind and solar. Still, the less electricity used, the better for the environment.

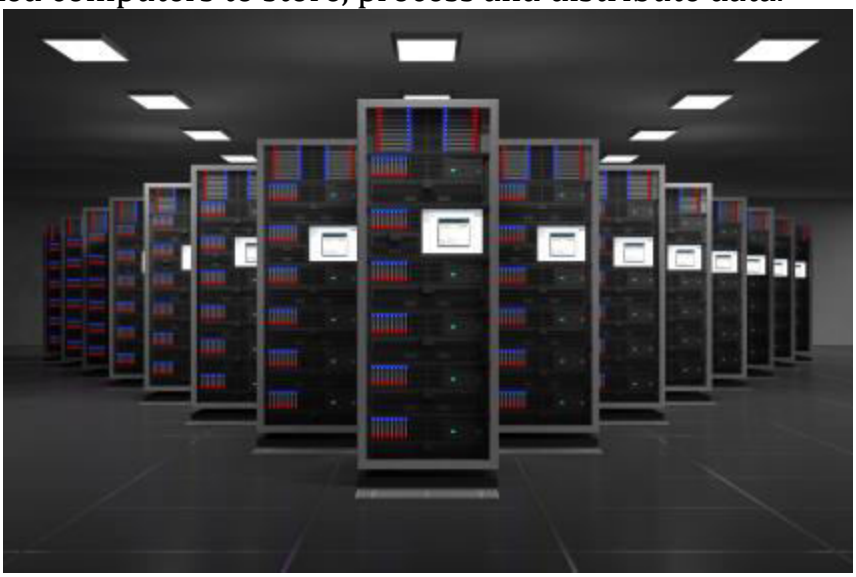
How Technology can help reduce energy use

- Many modern buildings have computer controlled systems in place that reduce the amount of energy they use.
- Solar panels to reduce the amount of electricity from the national grid

- Energy monitoring displays to help staff know what is using up the power
- Low energy LED lighting controls
- Water conservation systems to re-use water, especially in industrial factories
- Smart meters to help people at home keep track of their energy usage

Environmental topics

6. Data centres

- Data centres are facilities used to house an organisation's IT operations and equipment. They can contain hundreds, even thousands of networked computers to store, process and distribute data.
- 
- Data centres use a lot of energy to run the machines. They also generate a lot of heat, which requires even more power to manage. Data centres use about 3% of the global electricity supply, and is estimated to treble in the next decade. This will have a huge impact on greenhouse gas emissions.
- They impact the environment in other ways, too. The buildings housing them need huge amounts of concrete, copper cabling and other materials. Often data centres are located in remote areas, requiring road extension and maintenance, and increasing the fuel consumption of employees. The computer components include rare and valuable materials.
- E-waste is also an issue. To prevent downtime even with heavy use, the machines are replaced even when they still have plenty of 'life left in them'

- Our consumption of online content is increasing, requiring ever more and ever larger data centres. Is there a case for rationing access to data in order to reduce the impact on our environment?

Environmental topics

7. Monitoring the Earth and its habitats

Our planet is now monitored 24/7 as never before. This is because of our increasing concern about our environment and climate change.

We use technology such as satellites, sensors and weather stations, to monitor and measure changes in the local and global environment. Some of the things which are monitored include the:

- state of the polar ice over time
- flow of ocean currents
- changing temperatures of the oceans
- alarming growth of deserts
- burning of primary jungles such as the Amazon
- tracking endangered species for conservationists
- state of crops and greenery around the planet

The reason for all this monitoring is that nations may then agree on the best way forward (or it seems more likely they disagree!) But at least the scientific data is there for them to argue over.

Environmental topics

8. Stakeholders

All of the issues discussed in these sections are viewed differently by different interest groups. The UK government is going to be concerned about very different things to the governments of developing countries, or to manufacturers of electronic devices, or even to the general public.

Each of these groups are *stakeholders*, in that they have a stake in the issue being discussed. You will be asked on the exam to consider scenarios from the viewpoints of different stakeholders. Who those stakeholders are will vary from issue to issue, but as a jumping-off point you can consider three: the **British government**, the **British public** and **British industry**. Other stakeholders for the environment, for example, might include environmental activists, foreign governments, international energy suppliers, etc.

The British Government and the Environment

From the government's perspective they will want to ensure that the British economy keeps up with new technology. If we were to fall behind other countries this could have a huge impact on our ability to be competitive in the world markets.

The government will want to ensure that we are not totally reliant on other nations for our energy needs, especially when they can put prices up or limit supplies

The government will also be concerned with ensuring that the environment around the British isle is not damaged because of the impact we are having on our environment. Issues such as climate change, rising sea levels, burning fossil fuels etc will be something that they will monitor.

The government will also be responsible for ensuring that legislation and/or guidelines about recycling and e-waste are adhered to. The culture nowadays is to throw perfectly usable technology away. However, we can't keep throwing things away, landfill sites are already becoming overfull. So the government are trying hard to enforce strict recycling policies.

Environmental topics

9. Stakeholders - corporations

The legislation which is in place to help protect the environment makes manufacturing more expensive.

Businesses are not allowed to pollute the atmosphere with dangerous waste/chemicals. They have to dispose of all hazardous material in a safe manner. They must also have recycling policies in place and ensure that the whole business abides by them.

All of this costs money which lowers profits and can make products more expensive than similar ones that have been imported from countries that do not abide by the same rules.

On the plus side, the demand for more eco-friendly solutions does open up new markets for businesses.

Environmental topics

10. Stakeholders - individuals

The environmental legislation imposed on businesses means that their higher manufacturing costs have to be passed on to the consumer. Individuals therefore end up paying more for items that are produced by companies who abide by the legislation.

Many individuals care about the environment and many now recycle as much as possible. They want to ensure that future generations will have a pleasant and safe environment in which to live. It does take time to recycle, especially if a trip to a land-fill site is needed.

However, many individuals still have a blinkered view and only think about the 'here and now'. They see a new gadget and want it. They don't have any concept about the impact that the manufacturing process has on the environment. And they don't really think about the impact of e-waste.

Environmental topics

11. Summary

- People produce a lot of computer waste by throwing away their working devices. This is called E-Waste
- Less E-Waste can end up in landfills using three strategies: Reduce, Reuse, and Recycle.

- Computer systems can reduce E-waste by making manufacturing more efficient. Individuals can reduce e-waste by holding on to their old devices

- Old devices can be re-used by others. Computer systems increases the amount of re-use going on by making it easier for sellers to find buyers, and by making it easier to coordinate donation efforts.

- Broken devices can be recycled, with their material going into new products.

- Computers use a lot of energy. But computer systems can help reduce the amount of electricity required by identifying where it is being used through smart monitoring and more environmentally-friendly energy generation.

- The state of the environment is being constantly monitored, giving policy-makers better information about how to go forward. Conservationists receive more tracking information about endangered species than ever before.

Privacy topics

1. Introduction

Technology of itself is neither good nor bad. For example an axe is a great tool for cutting wood or it can be a nasty weapon. It is simply how people choose to use technology that can sometimes cause concern.

One of the key issues in society is the balance to be struck between a citizen's right to privacy and a governments' obligation to keep its country safe and secure.

Computing technology has a huge impact on this issue.

This theory section introduces you to some of the issues that technology has brought about. There are no right or wrong answer to many of the topics.

As an informed citizen it is up to you to have your own opinion.

Privacy topics

2. DNA Profiling

Every person has a unique DNA profile.

Ever since 1995, the UK police have built up the largest DNA database in the world. By 2015, it held over 5.7 million records. One in every eleven UK residents are recorded in the database.

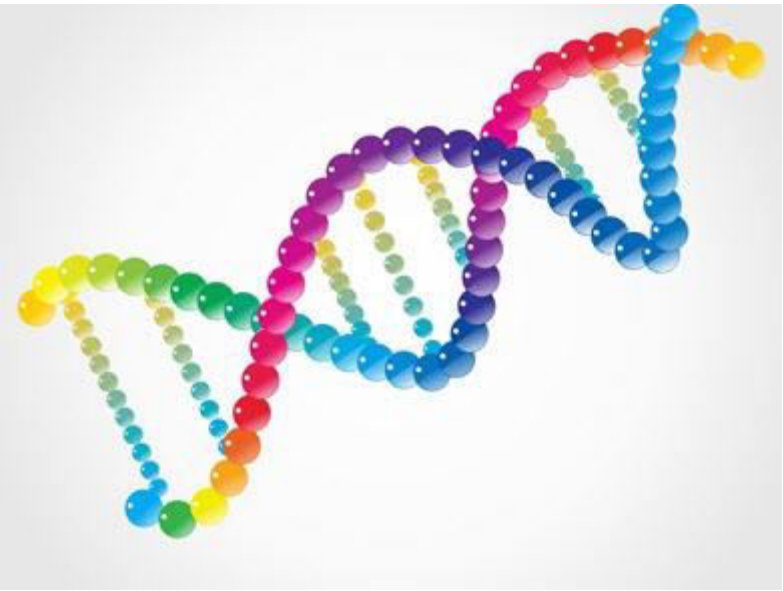
Just like the fingerprint database, as more records are added, it makes it that much more likely that a crime is solved with the help of this database

Keeping a DNA record of all criminals to solve future (or past) crime seems to make sense.

But consider these situations:

- A person is found innocent of the crime - should their record be erased from the database?
- A person has been found guilty of a minor offence. Should they remain on record for ever?
- Should we go the whole hog and keep a DNA profile of every person in the UK including new born babies?
- Should we have a DNA record of every visitor that comes to the country?

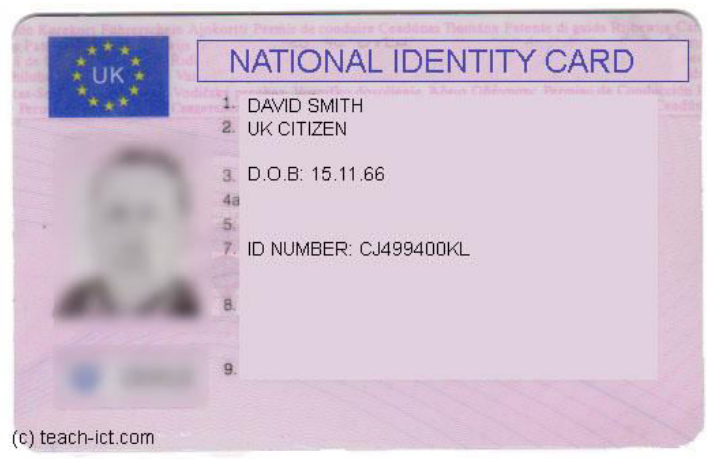
What do you think? What is the balance?



Privacy topics

3. National Identity Cards

Many countries around the world, from Argentina to Turkey to South Africa, require their citizens to carry around identification papers.



There has been an ongoing debate about whether to adopt such a policy in the UK. And, if we did, whether to make use of the latest technology to ensure that everyone can be uniquely identified. Biometric data such as fingerprints would be included in the card, along with a photograph registered in a national database.

There is no real technical barrier to do this, after all every new UK passport has similar technology.

The controversy lies in the right of the innocent citizen to privacy and why should they be forced to carry around such a card.

Argument for:

- It is argued that it will reduce crime and terrorism.
- It will also be convenient for opening bank accounts and so on as proof of identity.
- No need to carry other forms of ID e.g. driving licence or passport

Argument against:

- Citizens should not have to prove who they are wherever, whenever
- We already have documents to prove ID - passport, driving licence, so why another one
- It is expensive. Why should we pay for yet another document
- It may not be secure - there is a chance of fake ID cards being used for identity theft
- Used for surveillance - further erosion of privacy
- Risk of it being scanned and cloned, much like bank cards are today.

For now, the idea of a national identity card in the UK has been shelved. But it may be revisited by a future government.

Privacy topics

4. CCTV - Closed Circuit Television

The UK has more cameras pointing at its citizens than any other country in the world. More than a million cameras are connected to video recorders situated in control rooms dotted around the country.

A CCTV camera is often seen mounted up on street corners, car parks, shops. People are so used to seeing them that they tolerate them and for the most part probably don't even notice them.

Recent technology has enabled the images obtained from CCTV to be combined with other systems that recognise faces (facial recognition systems) and those that identify number plates (automatic number plate recognition).

The argument for them is that:

- they reduce crime in the street
- they reduce theft from shops
- they improve safety and security

Some questions:

- How far should this surveillance go?
- Do you want strangers to know where you are at all times?
- Do you trust them not to misuse the information?
- Do they actually reduce crime or simply move it elsewhere?

They are now starting to appear in our places of work. Is this an invasion of privacy? Should ordinary managers have the right to use CCTV to monitor their workers?

Cameras are also appearing in school classrooms. Is it right that teachers and students are monitored in the classroom?

Once again it is a balance of the right of the citizen to privacy against their effect on potential wrongdoing.

Privacy topics

5. Electronic tracking

Many of the electronic devices that you carry around day-to-day are constantly sending out radio signals declaring their location.

Your mobile phone needs to do this in order to be assigned to a particular cell in the phone network, for example. Even devices that don't broadcast your location all the time, can give your location away when you use them. Your bank will keep records of wherever your credit card was used to make a purchase, for example.

This location tracking isn't necessarily bad - your phone wouldn't even work without location data. But what if this information is used for reasons other than their original purpose? If someone put all of this location data together, they could make a complete map of your movements throughout the day.

This is where the controversy lies.

Which authorities have the right to access these records? For what reason?

For example, is it right that a local council uses electronic tracking tools designed to counter terrorism in order to spy on suspected dog fouling?

The risk to citizen privacy is 'mission creep' where strong systems and laws set up to counter serious crime are used for trivial reasons.

Privacy topics

6. Personal data

Your personal information has a cash value. Advertisers and marketers are always looking to learn more about potential customers. Criminals want to impersonate you for fraud. Researchers and sociologists want to learn more about how different demographics respond to various things.

With the development of social media technology and with companies sharing data about their customers with each other, it is easier than ever to put together profiles about people. In many cases the individuals themselves will freely share their personal information. Watch this video demonstrating how easy it is for strangers to find out your personal information from just a Facebook Like. You will need YouTube access to view it.

This compilation and sharing of data poses a great risk to individual privacy, and new technologies are coming out all the time to help collect and tie together more information. Laws such as the Data Protection Act limit what data companies are allowed to keep about their customers and for how long, but it is up to every one of us to be more aware about how much we are saying about ourselves to strangers.

Privacy topics

7. Stakeholders: Government

You may be asked in your examination to consider scenarios from the viewpoints of different stakeholders. Who those stakeholders are will vary from issue to issue, but a good starting point is to think about these three: the **British government**, the **British public** and **British industry/ organisations**. Depending on the specific scenario you are given you might also need to consider stakeholders such as environmental activists, foreign governments, international energy suppliers, etc.

The British Government and Privacy

The government is responsible for protecting the countries' people, industry and infrastructure . In previous centuries, that mostly meant against other nation-states, but national threats in the modern world are on a different scale. Technology has given *individuals* the power to cause great harm, i.e. terrorist attacks, cyber attacks, crime etc.

To fight such threats, the government needs to identify and monitor anyone they consider might pose a threat. Surveillance cameras, DNA databases and

national identity cards mean that people can be tracked and monitored. Communications by e-mail and telephone can be recorded and scanned for keywords. Tracking data from mobile phones can indicate someone's presence at a crime scene.

You might ask yourself whether the Government has the right to monitor us so closely. On the other hand, how safe would we be without this type of intervention? The Government has to maintain a delicate balance between the two.

The Internet has proven to be a powerful platform for social change. People openly (and privately) discuss things that can affect society at large. People have been radicalised, social uprisings have been arranged and criminal activity is commonplace.

No one owns the internet, so no one is officially in charge of policing it. Despite this, the UK government take steps to monitor and censor certain types of internet traffic. They constantly scan internet chatter looking for evidence of criminal and terrorist activity. People have been known to get a visit from the police in the middle of the night after posting a drunken tweet to the effect that they are 'going to kill their boss'. Are government bodies such as the police, right to undertake such monitoring, after all, it is our private communications that are being examined. Or do you think they are doing the right thing in order to keep everyone safe?

Privacy topics

8. Stakeholders: Corporations

Most businesses are concerned with making money - after all, that is how they exist. To make money they need to sell things to us, and they get our attention through adverts on TV, radio and in magazines. However, advertising is expensive and so marketers are focusing on how they can target the exact people who might be interested in their products.

Have you noticed that when you look for something online, not long afterwards you will start seeing adverts for that type of product appear wherever you go online? This is done by placing cookies on your computer which monitor the sites that you visit or keywords that you type. Is this an invasion of our privacy or something aimed at helping us find things we need? Should organisations be able to track what we are looking at?

When we fill in an online form or sign up to a website, we give away a lot of personal information. Often this information is then sold on to organisations who use it to send us targetted adverts. Should our data be sold on? Should

organisations be able to buy and use this data? Do you believe that targetted adverts are beneficial for us?

The rise of "Big Data" gives corporations more information about the public than ever before. this information is bought, sold, and compiled, and used by large corporations to decide on the direction they should take with new products for the next few years.

On the other hand, privacy issues can affect organisations themselves. When bidding for a contract they may have to declare any conflict of interests. This means giving releasing data that might otherwise be private.

Limited companies have to publish their financial records. This enables competitors to view their financial information - does that affect their privacy?

Privacy topics

9. Stakeholders: Individuals

Privacy is a basic human right. It is not something that has to be "earned" or that should be traded away. Rather than arguing why someone *shouldn't* be required to carry a national identity card, privacy advocates demand that the government make its case that they *should*, and have found most arguments unconvincing so far.

Britain is already the most surveilled nation in the world, and has the largest DNA database. Laws are in place to monitor our internet traffic and our phone conversations.

And yet it seems that no matter how much privacy is given away, nothing seems to change. No more terrorists are caught now than before, yet the

government continue to promise that giving away *just a little more* of our private data will help make the country safe again.

There has been an increasing backlash and resistance against invasions of privacy. Revelations by whistleblowers at intelligence agencies have shown how much of our daily lives is being monitored and recorded.

Still, many of the public agree that some degree of privacy is worth sacrificing if it keeps us safe. Others are completely unconcerned, and put up their entire lives for everyone to see through social media, personal weblogs and video blogs.

Privacy topics

10. Summary

- Technology has helped to erode personal privacy in many ways
- Police keep a database of DNA profiles of criminals and suspected criminals
- Government-issued National Identity Cards can incorporate biometric data for better tracking
- Closed circuit television cameras can track people as they move around a town or city
- Your electronic devices provide constant updates on your location
- Personal data is valuable to many different groups
- People give away their personal data all the time through social media

Cultural topics

1. Introduction

Technology has always had an impact on human culture, for example the printing press made it cheaper and easier to spread knowledge and beliefs.

And with the rise of the Internet, it has never been easier to spread the values of a culture to other people around the world.

And yet despite this incredible benefit, it has some downsides as well. Think of these questions:

- Is there a digital divide, where some have access and others do not?
- Are some people engaging in obnoxious behaviour online, something they would not dare do face to face?
- Does being online so much lead to fewer friends and experiences in real life?
- Can dangerous ideas and beliefs be spread too easily?

This section will cover some of the technologies that have most impacted culture in the West. However, this is such a broad topic and we can't possibly cover every angle. We suggest that you try to keep up-to-date with technology news stories and think about the impact that different examples have on their relative stakeholders.

Cultural topics

2. Anonymous culture

Is being able to be anonymous on the Internet a good or bad thing?

Is it right that someone can send hateful messages without any comeback?

On the other hand is it right that if people can't have anonymity when they need it, they may be afraid to point out an injustice as activists often do. Or they are afraid of revealing an illegal act as whistle blowers are afraid of retribution?

The Internet can provide a platform to say things that are not socially acceptable in certain cultures, for example being gay is illegal in some countries and even discussing it would lead to prosecution. Anonymity provides a shield to shelter behind.

At the same time, there are many critics of online anonymity.

Hackers can trick you into giving up your personal information by pretending to be someone that they are not. Spammers can send out advertisements from anonymous e-mail addresses without worrying about complaints.

Governments have put laws in place (RIPA for example) to help identify persons if they are behaving illegally. For example in the UK, internet service providers now have to keep 12 month records of a customer's connection and search history - which web sites they visited, how long for, what they did then, and so on. And the authorities do not need a warrant to access those records.

Protecting against the downsides of anonymity does, however, mean losing some of the benefits.

Cultural topics

3. Social networking

Almost everyone in the UK is connected to one social media network or another. Facebook, Twitter, Snapchat, Instagram etc. Social networking sites allow people to communicate with one another more easily than ever before. Organising group activities, sharing information, or just having a chat are all good reasons to keep logging on.

Social networking allows businesses to advertise to customers, receive feedback and respond to comments in real-time.

Social networking enables the government, police, and health services to release up-to-date bulletins to citizens about ongoing emergencies. The information contained in social networks can be used to track down criminals or missing persons, to evaluate potential new employees or employers, and even romantic partners.

But social media also has a dark side. False information and fake news can spread just as quickly as real data, and can make it much more difficult for someone to work out the truth of a situation.

People can be distracted by social media to such a degree that it impacts on their education or employment. Others use it as a substitute for real human friendships, steadily becoming more isolated from the community around them.

And, just as social media can help individuals find positive and affirming groups, it can also provide a banner for hate groups and extremists to organise themselves around.

In the end, social networking is one of the most powerful tools developed for the Internet, and it has profoundly affected every culture interacting online in one fashion or another.

Cultural topics

4. Health effects

Computing technology has had a huge impact on medicine and health services. People are living longer and healthier lives than ever before, and this will have a great impact on society in the upcoming decades.

Access to online journals allows doctors to keep up with the latest developments. Developments in new diagnostic and scanning technology has helped speed up and improve the accuracy of diagnosing a whole range of different diseases.

Computer modelling techniques make it possible to determine how diseases will spread in a population and how particular drugs might provide the best treatment options.

Genetic profiling identifies risk factors well in advance of any symptoms.

But more relevant to a discussion on culture and technology is the effect that computing technology has on the individuals using it. Extensive use of social networking sites has been shown to physically "re-wire" the frontal cortex in the brain. Social media "addicts" often show a stronger need for instant gratification, a reduced attention span, and decreased ability to hold conversations in person. Personality disorders and addiction issues are more likely, and many more report feeling lonely, depressed or anxious in their day-to-day lives, especially at times when they are unable to access social media.

Likewise, the shift to a computer-based office where workers sit unmoving at their desks for hours upon hours has led to an increase in certain types of physical ailments such as repetitive stress injury (RSI), lower back pain, headaches and eye strain.

These problems can be lessened or eliminated by taking a more healthy approach to computer use and ensuring that you take frequent breaks away from the computer and adopt a healthier posture while sitting at your desk.

Cultural topics

5. Citizen journalism

Before the days of the Internet, anyone wanting to report the news faced huge startup costs in printing and distributing their material to potential audiences. Nowadays, all someone needs is a blog (often free to set up), a social networking account and a desire to get your voice heard.

Established news organisations have found it difficult to compete with the rise of this so-called "citizen journalism". Unable to compete with "free" on price, broadsheets are forced to compete on quality and reputation.

Citizen journalists have the advantages of lower production cost and higher responsiveness to local news - often the most interesting news for a local audience. They can often pick up on stories that would otherwise be missed. Any stories they break that affect a larger audience can then be re-written and re-reported in larger publications.

The lack of editorial oversight can make for a more individual voice, and fewer restrictions on what a citizen journalist can report on. Online blogs and journals offer many different perspectives but also results in lower quality fact-checking and presentation.

Citizen journalists often have little training in the ethical and professional duties of reporting, and fewer professional contacts to draw upon to provide context to what they dig up.

No-one agrees on whether or not citizen journalism is poised to replace mainstream media entirely or whether it should be used to supplement established news brands. Maybe it's just a fad which is likely to fade as people turn back to more reliable sources, but we don't think that is going to be the case.

Cultural topics

6. Viral videos

Viral videos, images, and other "memes" can spread very rapidly across the internet. Some are hilarious - think of the mum sat her car trying on the chewbacca mask:

What about the baby panda that sneezed and frightened its mum? We are sure that you can think of many other videos that have unexpectedly gone viral.

What these viral videos have in common is that they draw in huge numbers of people. They give people across the world a shared experience that they can discuss or build upon together.

People can become celebrities overnight because a video they have made has gone viral. Most get their 10 seconds of fame and then fade away into obscurity as soon as the next viral video comes along.

Advertising companies try to manufacture viral media in the hope of gaining huge amounts of free publicity for their products. Social movements can spring up in response to single videos and bring about substantial political and legal changes.

The public image of politicians and other elites can be raised or lowered by appearances on viral media, to the point where election campaigns have begun to try to get ahead of or harness viral media to create a brand for their candidate.

Even individuals try to get in on the action, leading to any mildly interesting or remarkable event is instantly captured on a cellphone camera by someone

looking to upload it later. People can spend huge amounts of time and money in search of creating the perfect viral video. The trouble that ultimately, no one really knows what will make a video go viral.

1. Introduction

Over the past few decades, computers have become ever more important in our day to day lives. Things that the law had never previously had to consider began to crop up. For example, online fraud, hacking and the sheer amount of personal information that we readily, and happily share over the internet.

New laws were written and old laws were updated to better govern and control the use of technology and access to data.

For this syllabus, the topics you need to know about are:

- The Data Protection Act (2018)
- The Computer Misuse Act (1990)
- The Copyright, Designs, and Patents Act (1988)
- Software licences - open source and proprietary

2. Data Protection Act (2018)

Computers are capable of holding and organising vast amounts of data, far more than was possible using older paper-based systems. In years past, someone would need to go through endless filing cabinets to find information on a single person. Now, a computer database allows instant access to any data collected on an individual.

The power of such databases and the potential for misuse is why Parliament passed the Data Protection Act in 1998 and has now been updated in 2018 to include the new European GDPR, General Data Protection Regulation.

The Act sets out rules for handling other peoples' personal data.

The DPA requires that every data controller (i.e. every organisation or sole trader) who wants to collect or process personal data must register with the Information Commissioners Office. They have to disclose what type of data they are collecting and why they are collecting it.

Sensitive data such as race, criminal background, or religious beliefs have even more restrictions placed on their collection.

Exemptions

Although the Act states that everyone who collects and uses personal data must register, there are a few exemptions to this rule:

National Security - If required for the purpose of safeguarding national security, the government does not have to disclose what data they are holding about individuals.
Crime - Data which is being held in order to prevent or detect a crime does not have to be disclosed.
Taxation - any data collected for taxation purposes is exempt

3. The Eight Principles of the DPA

While the details of the Data Protection Act can get quite complicated, the intentions of the Act can be summed up in eight "Principles".

The Eight Principles are as follows:

Eight Principles

Principles	What it actually means
1. Personal data should be obtained and processed fairly and lawfully	This means that you should be told about data which is being collected about you and should be asked for your permission to collect it. You should also be made aware of the reason why the data is to be collected and for what it will be used.
2. Personal data can be held only for specified and lawful purposes	The data collector has to state why they want to collect and store information when they apply for permission to be able to do so. If they use the data they have collected for other purposes, they are breaking the law.
3. Personal data should be adequate, relevant and not excessive for the required purpose	Organisations should only collect the data that they need and no more. Your school needs to know your parent's phone number in case they need to contact them in an emergency. However, they do not need to know what your grandmother's name is, nor do they need to know your eye colour. They should not ask, nor should they store such details since this would be excessive and would not be required to help with your education.

Eight Principles

Principles	What it actually means
4. Personal data should be accurate and kept up-to-date	Companies should do their best to make sure that they do not record the wrong facts about a data subject. Your school probably asks your parents to check a form once a year to make sure that the phone number and address on the school system is still correct. If a person asks for the information to be changed, the company should comply if it can be proved that the information is indeed incorrect.
5. Personal data should not be kept for longer than is necessary	Organisations should only keep personal data for a reasonable length of time. Hospitals might need to keep patient records for 25 years or more, that is acceptable since they may need that information to treat an illness later on. However, there is no need for a personnel department to keep the application forms of unsuccessful job applicants.
6. Data must be processed in accordance with the rights of the data subject	People have the right to inspect the information held on them (except in certain circumstance - see later).

Eight Principles	
Principles	**What it actually means**
	If the data being held on them is incorrect, they have the right to have it changed.
7. Appropriate security measures must be taken against unauthorised access	This means information has to be kept safe from hackers and employees who don't have rights to see it. Data must also be safeguarded against accidental loss.
8. Personal data cannot be transferred to countries outside the EU unless the country has similar legislation to the Data Protection Act	This means that if a company wishes to share data with an organisation in a different country, that country must have similar laws to our Data Protection Act in place.

4. General Data Protection Regulation (2018)

The Data Protection Act (2018) described on the previous page is a UK-based law. A new European regulation came into force in 2018 that applies to the European Union. It is abbreviated the GDPR.

It is very similar to the Data Protection Act but it has some important new rights - namely the right to be forgotten, formally called 'the right to erasure'. Social media and search engines are now an important part of many peoples' lives. But do they really need to retain a record of that embarrassing posting or damaging event, forever?

The second major change is that individuals will now have the right to contest decisions made through artificial intelligence or computer algorithms. Consumers will be able to insist that a human is involved in the decision-making.

In summary, these are the individual rights

Individual Rights

Principles	What it actually means
1. The right to be informed	If an organisation or web site is collecting information about you, then they need to explain what they are doing with the collected data and make it easily understood. This is often set out in their privacy policy.
2. Right of access	Each person has the right to see what personal information is being held by the organisation
3. Right to remedy	If the personal information being held is inaccurate or incorrect then each person has the right to insist that it is fixed.
4. Right to erasure	This is the right to 'be forgotten'. The main idea is that each person can insist that their personal data (including postings etc) are deleted where there is no compelling reason for its continued retention.
5. Right to restrict processing	The individual has a right to 'block' further processing. For example if the personal data was obtained for one reason such as admin of an account, then it can be blocked from being re-sold to a third party for other uses.
6. Right to data portability	Each person has the right to obtain and re-use their personal data for their own purposes across different services. For example consumers can take advantage of apps and services to find them a better deal or help them understand their spending habits.

Individual Rights	
Principles	**What it actually means**
7. Right to object	Each person has the right to object to how their personal data is being processed. For example it is being used for direct marketing or personal profiling.
8. Rights related to automated decision making including profiling.	There is a famous comedy sketch where an official is droning to the customer 'The computer says no" without a care. This is an example of a decision being made by an algorithm based on your personal profile. Now individuals have the right not to be subject to an automated decision, they can insist on human intervention and/or an explanation of the decision and challenge it.

5. Computer Misuse Act (1990)

Hacking has been around almost as long as the Internet; some people just love to try and break into a computer system.

In the early days, there was no legislation in place to tackle the problems caused by hacking. Everyone knew that it was wrong, but it wasn't illegal and so there was nothing that the police could do even if a hacker was caught.

So in 1990, the Computer Misuse Act was passed. This made it illegal to break into someone else's computer to steal, edit, or delete data.

The Computer Misuse Act recognised the following new offences:

1. Unauthorised access to computer material
2. Unauthorised access with intent to commit or facilitate a crime
3. Unauthorised modification of computer material.
4. Making, supplying or obtaining anything which can be used in computer misuse offences.

Or in short:

1. Accessing computers without permission
2. Modifying data without permission
3. Creating or supplying malware

The Act was amended in 2014 to include up to a 10 year prison sentence for the most serious computer related crimes. (see here, have a look at item (6) part (c))

6. Copyright, Design, and Patents Act (1988)

Computers have made it very easy to copy material, whether it be text, images, music, or videos. This is great for people selling their work, but it also means that people can steal work more easily.

In order to protect the investment of time, money and effort by the people who create original pieces of work, the Copyright, Design and Patents Act (1988) was introduced.

The purpose of the Act was twofold:

1. To allow people or companies creating media, to be paid for the effort they had to put into creating the work.
2. To protect the "Intellectual Property" rights of the creator. This means that the creator can decide how their work is copied, or even if it can be copied at all.

The 1988 Act grants an automatic 'copyright' to anyone who has published a **creative** work, whether that work is digital or physical. Examples of works that would be covered by copyright include artwork, stories, music, and poetry. Other people cannot share copyrighted work without the permission of the creator.

Copyright lengths vary from country to country, but the most common length (and the one used in the UK) is 70 years after the author's death. So a piece of music someone wrote when they were 18 years old is likely to remain copyrighted for over a century.

Because copyright is automatic, creators do **not** need to warn people that they cannot copy the work.

7. Copyright and 'I didn't know'

If you do any of the following, you are breaking copyright law:

- copying commercial software (i.e. software you should have paid for)
- copying or downloading music or films (that should you should have paid for)
- copying an image from a web page. If you find an image using Google, you should NOT use it without first asking for the owner's permission.

- copying text from a webpage and using it as your own work

" I didn't know so I'm not guilty"

You won't get way with saying 'I'm sorry, I didn't know'. If you copy things and pass them off as your own, you are guilty of breaching Copyright..

"If it doesn't have a copyright notice, it is not copyrighted."

Nope, you won't get away with this one either. Any original work is copyright, whether it has a copyright notice on or not. If something looks copyright then you should assume that it is.

"If I don't charge for it, I can copy it'
False. It doesn't matter if you charge someone or not, copying is copying is copying, whichever way you look at it.

Breaking the copyright laws can result in very heavy penalties - you can get a hefty fine and even get sent to jail!

Don't think that it can't happen to you - it can. Many organisations, quite rightly, fiercly protect their work and they will prosecute you if they catch you!

8. Proprietary software licence

Commercial software is owned by a business who has invested time and resources for it. The business has the 'intellectual property' rights to it.

Intellectual property is usually handled legally with a proprietary licence.

Creators receive an automatic copyright over anything they write. But since it is so easy to copy source code and take it apart to find out how it works, anyone publishing the source code to their software risks having someone else steal, modify, and sell it for themselves.

The solution to this is to not publish the source code itself, but to compile it into a set of machine code instructions in an executable file, and rent that file to customers.

Note the word 'rent' - when you purchase software, you do not actually own it. What you have done is to enter a contract with the seller that gives you permission to use it in a certain way, it might even be time-limited so that you have to pay an annual fee to keep using it. These permissions are set out in a document called a 'licence'.

A single-user licence states that only one person can use it at any given time. Multi-user licences are usually much more expensive. The licence usually forbids copying or reverse engineering the code and this is covered by the data protection act.

Benefits of a proprietary licence

Commercial applications tend to be quite polished compared to an equivalent "open source" application. Documentation and help tends to be better as well. After all, they want to attract as many customers as possible. Open source does not have this pressure to be as user friendly.

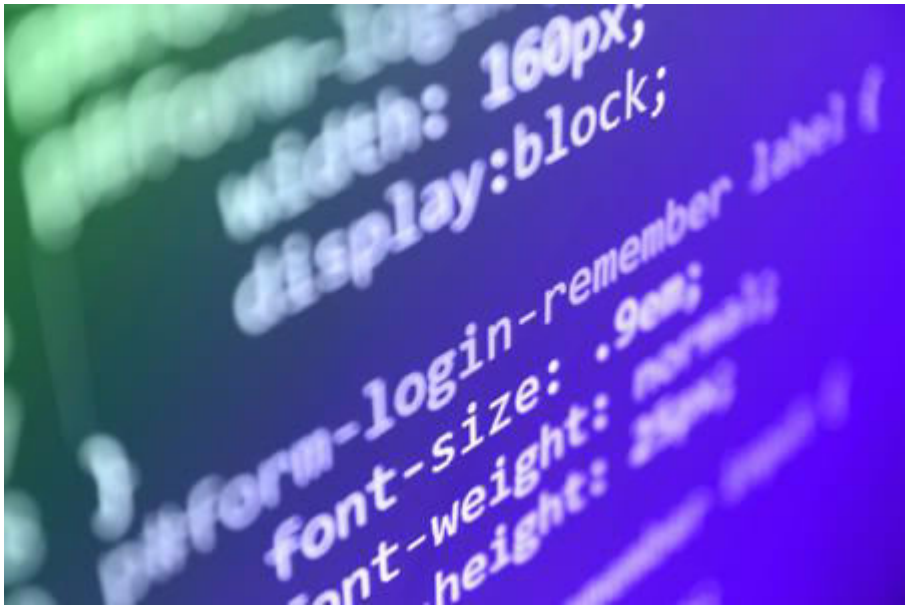
They also offer formal support in the form of regular software updates and perhaps direct customer support for a specific period after purchase. If the

customer needs continued support, then they may be able to set up a support contract with the vendor.

9. Open source software

With open source, the source code itself is available to the public. Anyone with the right skills can compile the source code to create the applications' executable file. The source code is free.

People may make their software open source either out of a sense of altruism. Or perhaps they want their work to be used by as many people as possible. Alternatively it may be because they want to make it possible for others to collaborate and build upon what they have created.



Many licences have been developed to support open source distribution. For example the GNU General Public Licence in summary is shown below

You may copy, distribute and modify the software as long as you track changes/dates in source files. Any modifications to or software including (via compiler) GPL-licensed code must also be made available under the GPL along with build & install instructions.

So if you modify the source code then that version also has to be made available under the GNU licence.

Open source code is written by volunteers - experts in their field who want to make their code available. Just like their commercial counterparts, they need somewhere to work together online, and so services such as SourceForge provide a centralised online environment to support open-source projects. GitHub is also very popular depository of projects.

Here are some examples of open source software

- GIMP - a photo editing application
- Open Office - an office suite with word processor, spreadsheet and database
- Audacity - an audio recording and editing application
- Linux - operating system