7 Ethics and ownership

In this chapter, you will learn about
- the need for and purpose of ethics as a computer science professional
- the need to act ethically at all times
- the impact of acting ethically or unethically in a given situation
- the need for copyright legislation
- the different types of software licensing, including free software, open source software, shareware and commercial software
- the impact of artificial intelligence (AI) on social, economic and environmental issues.

WHAT YOU SHOULD ALREADY KNOW

Try these four questions before you read this chapter.

1 a) What is meant by an *expert system*?
   b) Name **four** components of a typical expert system.
   c) Give **three** examples of the use of an expert system.

2 a) What is meant by *copyright*?
   b) Why is copyright important?
   c) Give examples of items which would be covered by copyright laws.
   d) Differentiate between the terms *plagiarism* and *copyright*.

3 a) What impact do computers have on the general public with regards to

      i)   jobs/employment
      ii) the environment
      iii) how we shop and bank
      iv) human interactions?

   b) Describe **three** positive aspects of the impact of computers on society.

4 What is the influence of social media on
   a) news reporting
   b) world safety
   c) personal and private lives of people
   d) politics?

7.1 Legal, moral, ethical and cultural implications

The following definitions are important when considering ethical behaviour:

- **Legal** covers the law, whether or not an action is punishable by law.
- **Morality** concerns questions of right and wrong, and is more often thought of in relation to personal or individual choices.
- **Ethics** also concerns questions of right and wrong, but is more often used in a professional context.
- **Culture** refers to the attitudes, values and practices shared by a society or group of people.

Anything which breaks the law is termed illegal. Examples include copying software and then selling it without the permission of the copyright holders (see Section 7.2).

Morality is the human desire to distinguish between right and wrong. This varies from person to person, and between cultures (something that is considered immoral in one culture, may be acceptable practice in another, for example).

Immoral does not mean something is illegal (and vice versa). Creating a fake news website, for example, is not illegal, but it may be considered immoral if it causes distress to others. If the creator tried to obtain personal and financial data, then it would be become an illegal act.

Similarly, hacking is generally regarded as immoral, but not illegal. However, it becomes illegal

if it compromises national security, or results in financial gain, or reveals personal information, for example.

In short, there is a fine line between an immoral act and an illegal act.

Unethical behaviour is the breaking of a code of conduct. For example, if somebody works for a software company and passes on some ideas to a rival company, this would be regarded as unethical behaviour. If the software is related to national security or is formally copyrighted, then it is also illegal.

It is essential to be clear whether any law has been broken.

The importance of culture is less tangible. When writing computer games, for example, programmers need to be careful that they do not include items which some cultures would find offensive or obscene. Again, this may not be unethical or illegal, but could still cause distress. It is important to realise that boundaries can easily be crossed; in some countries making fun of religion, for example, is illegal.

7.1.1 Computer ethics

Computer ethics is a set of principles set out to regulate the use of computers. Three factors are considered:

- **Intellectual property rights**, for example, copying of software without the permission of the owner.
- **Privacy** issues, for example, hacking or any illegal access to another person's personal data.
- Effect of computers on society, for example, job losses, social impacts, and so on.

Internet use has led to an increase in **plagiarism** – this is when a person takes another person's idea or work and claims it was their own. While it is fine to quote another person's idea, it is essential that some acknowledgement is made so that the originator of the idea or work is known to others. This can be done by a series of references at the end of a document or footnotes on each page where a reference needs to be made. Software exists that can scan text and then look for examples of plagiarism by searching web pages on the internet.

7.1.2 Professional ethical bodies

There are a number of professional bodies representing individuals working in the fields of computing and information technology that have developed their own codes of conduct, to which members are expected to adhere. Belonging to one of these organisations demonstrates your professional integrity by showing that you are committed to upholding the standards they prescribe.

The British Computer Society (BCS)

The **British Computer Society (BCS)** is a professional body set up in the UK, initially to represent the rights and ethical practices of all professionals working in the IT and computing industries. It is now an international body which works in close partnership with other groups to monitor and advise IT practices across the globe.

The BCS Code of Conduct (www.bcs.org/category/6030) covers four main areas:

1 The Public Interest

2 Professional Competence and Integrity

3 Duty to Relevant Authority

4 Duty to the Profession

The Institute of Electrical and Electronics Engineers (IEEE)

The **Institute of Electrical and Electronics Engineers (IEEE)** was set up in the USA with the aims of

• raising awareness of ethical issues

• promoting ethical behaviour among professionals working in the electronics industry

• ensuring engineers and scientists respect the need for ethical behaviour.

To help in this aim, the IEEE has also set out a code of ethics:

IEEE Code of Ethics

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members, and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

1   to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, and to disclose promptly factors that might endanger the public or the environment;

2   to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;

3   to be honest and realistic in stating claims or estimates based on available data;

4   to reject bribery in all its forms;

5   to improve the understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies, including intelligent systems;

6   to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;

7   to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;

8   to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression;

9   to avoid injuring others, their property, reputation, or employment by false or malicious action;

10 to assist colleagues and co-workers in their professional development and to support them in following this code of ethics.

Jointly with the **Association for Computing Machinery (ACM)**, the IEEE has also developed a set of eight principles which govern the code of ethics specifically among software engineers. The principles set out to ensure all engineers meet an acceptable and consistent code of ethics. There are certain expectations of the scientists and engineers from the general public as well as from their peers. The actual eight principles behind the code of ethics and professional practice were published way back in 1999.

An abridged version is shown below; a full version can be found at:

www.computer.org/web/education/code-of-ethics

Software Engineering Code of Ethics

1   PUBLIC – Software engineers shall act consistently with the public interest (contains 8 sub-clauses).

2   CLIENT AND EMPLOYER – Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest (contains 9 sub-clauses).

3   PRODUCT – Software engineers shall ensure that their products and related modifications meet the highest professional standards possible (contains 15 sub-clauses).

4   JUDGEMENT – Software engineers shall maintain integrity and independence in their professional judgement (contains 6 sub-clauses).

5   MANAGEMENT – Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance (contains 12 sub-clauses).

6   PROFESSION – Software engineers shall advance the integrity and reputation of the profession consistent with the public interest (contains 13 sub-clauses).

7   COLLEAGUES – Software engineers shall be fair to and supportive of their colleagues (contains 8 sub-clauses).

8   SELF – Software engineers shall participate in life-long learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession (contains 9 sub-clauses).

There are 80 clauses and sub-clauses in total. We shall consider one scenario and see how it fits into a selection of the clauses.

Mikhail works during the day for a software company called *EthicalGamz* developing new software in a number of applications. Mikhail is part of a large team of software engineers writing and testing new code. The team also do market research to help in their development of new software for the future. Much of the work is commercially sensitive and multiple layers of access exist to protect the company from unauthorised sharing of data.

In the evenings and at the weekend, Mikhail works for his own company, *MikhailSoft,* which produces software available to buy on the internet only. To save costs, Mikhail uses coding he helped develop for *EthicalGamz* in his own software. He also outsources some of the work to software engineers in other countries where the wages are much lower and ethics policies are more lax. This saves him a lot of time and money when producing his own software. Mikhail does not pay any licensing fees to *EthicalGamz* and makes no reference to any code used from that company in his own products.

We will now consider the ethical implications of the above scenario using the following sub-clauses from the Software Engineering Code of Ethics.

1.03   approve software only if they have a well-founded belief that it is safe, meets the specification and passes the appropriate tests and does not diminish the quality of life, diminish privacy or harm the environment;

There is an ethical issue here since the software written by personnel from other countries may not meet the specification requirements or appropriate tests. It could lead to any of the three factors being violated, for example, the software may contain spyware of which Mikhail is unaware.

2.02	not knowingly use software that is obtained or retained either illegally or unethically;

Mikhail has no control over the coding being developed by his overseas team, furthermore, using the coding from *EthicalGamz* is illegal use.

3.05	ensure an appropriate method is used for any project on which they work or propose to work;

Using external companies (in his own country or overseas) may be used at various steps in the production of Mikhail's own software. Unless he applies good managerial control, he will be unable to ensure methods used in projects are appropriate or fully ethical in their implementation.

4.02	only endorse documents either prepared under their supervision or within their areas of competence and with which they are in agreement;

Documentation produced by third party developers is not produced under Mikhail's direct supervision, indeed some of the work done overseas may be outside Mikhail's sphere of knowledge which probably removes his ability to objectively endorse the external work being done.

5.03	ensure that software engineers know the employer's policies and procedures for protecting passwords, files and information that is confidential to the employer or to others;

By using software developed by *EthicalGamz* for his own use, Mikhail may need to give passwords and access to other files to engineers working for his own company, *MikhailSoft*. This would allow non-authorised personnel access to files and information stored on *EthicalGamz* computer systems leading to a potential security breach.

6.05	not protect their own interest at the expense of the profession, client or employer;

By using coding from *EthicalGamz*, Mikhail is enhancing his own interests at the expense of the company and his colleagues at that company.

7.03	credit fully the work of others and refrain from taking undue credit;

By using coding from *EthicalGamz* illegally and unethically, and by making no reference to the source of his 'illegal' code, Mikhail is effectively taking full credit for all the work done by his colleagues.

8.07	do not give unfair treatment to anyone because of any irrelevant prejudices

Mikhail may dismiss overseas workers who do not agree with his own political or religious beliefs and such dismissals would be deemed unfair and break this code of practice.

EXTENSION ACTIVITY 7A

Using the example above, consider the following eight sub-clauses and decide how (or if) Mikhail is breaking the code of ethics in each case.

1.01	accept full responsibility for their own work
2.03	use the property of a client or employer only in ways properly authorised, and with

the client's or employer's knowledge and consent

3.03   identify, define and address ethical, economic, cultural, legal and environmental issues related to work projects

4.04   not engage in deceptive financial practices such as bribery, double billing or other improper financial practices

5.02   ensure that software engineers are informed of standards before being held to them

6.08   take responsibility for detecting, correcting, and reporting errors in software and associated documents on which they work

7.02   assist colleagues in their professional development

8.09   recognise that personal violations of this Code are inconsistent with being a professional software engineer

7.1.3 Impact on the public

[Figure 7.1](#) summarises the potential impact of any software or hardware being developed on the general public.
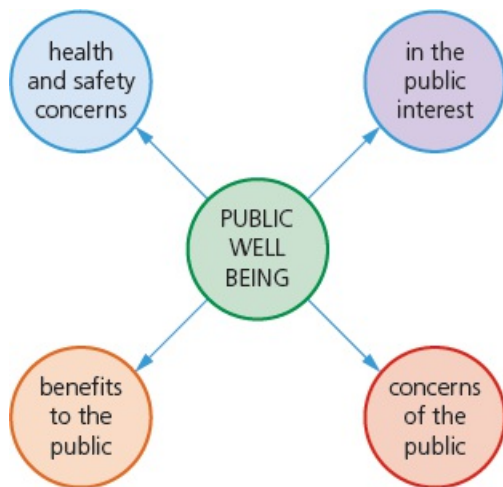

Figure 7.1 Potential impact of software or hardware being developed on the general public

While software engineers and scientists consider the Software Engineering Code of Ethics, the impact on the general public cannot be ignored.

This section begins by considering three instances in which computer hardware or software led to expensive errors, which impacted on the general public.

LA airport shutdown in 2007

In this example, aeroplanes at LA airport (in the USA) were grounded due to a simple software issue: a faulty network card in a device continued to send incorrect data over the airport's network. Eventually, the whole of the USA Customs and Borders Agency came to an abrupt standstill at LA airport. This resulted in all flights leaving and landing at the airport being cancelled for about eight hours until the fault was cleared. It cost several million US dollars in lost revenue to the aeroplane operators. The impact on the general public was cancellation of holidays, loss of business and general frustration.

Exploding laptop computers in 2008

Japan holds an annual trade show displaying the latest in computer technology. In 2008, during the trade show, a number of Dell laptop computers burst into flames under the full view of the visiting public and television cameras. The problem was traced back to faulty batteries in the laptops which had been overheating and eventually exploded and burst into flames. As if this was not enough, the problem escalated when Apple reported similar problems with some of its tablets, laptops and desktop computers. Some 100 million computer devices had to be recalled at an estimated cost of over 300 million US dollars to the manufacturers. The impact on the general public would have been devastating if this problem had not been discovered before the devices were generally available to buy.

Airbus A380 incompatible software issue in 2006

In Europe, Airbus Industries uses a number of factories throughout Europe where the design, development and construction of aeroplanes takes place. During 2006, while the new A380 was being developed, a surprising issue came to life: the software in two factories would not 'talk to each other'. The factory in Hamburg (Germany) was using an old version of CATIA design software while another plant in Toulouse (France) was using the latest version of CATIA software. When a part of the A380 from Hamburg and a part of the A380 from Toulouse were brought together for assembly, the wiring in the two parts did not match up (the cables could not be linked together). This was all due to the fact that the two versions of the software produced different design specifications for the wiring. It cost the company millions of Euros to redo the design and remanufacturing of parts where old software was still in use. Fortunately, this was not a safety issue, but if some other design incompatibility had

occurred after assembly of an A380, the effect could have been catastrophic leading to possible loss of life.

All of these examples are cost-related, but still had – or potentially had – an impact on the general public. Regrettably, there are many other examples. Other issues which can affect the general public and businesses include

- companies selling software systems which do not meet the required standard for security (inadequate protection against hacking, spyware and other security issues)
- the covering up of security issues (such as the XEN security threat which forced several cloud servers to become compromised – an attempt was made to cover up the issue but the affected cloud operators had to come clean)
- the release of private data (such as the celebrity photo leaks, when a cloud server was hacked)
- social media not policing subversive activity, such as hate mail and cyber bullying. Such activity is undergoing close scrutiny by several countries around the world
- search engines giving results at the top of the search due to donations to the search engine operators.

EXTENSION ACTIVITY 7B

Bearing in mind some of the issues raised above, consider these two questions.

1 Should we police the internet to stop certain activities taking place?
2 Should governments have the power to close down websites (such as *Twitter* or *Facebook*) which do not remove hate mail, incitements to violence or unacceptable photographs from their sites?

ACTIVITY 7A

1 Describe why it is necessary to produce a code of ethics to cover the computing and electronics industries.
2 Mariam and Asma were having a discussion about whether or not the internet should be policed.
   Mariam was in favour of the argument and put forward two reasons.
   ① It would prevent illegal material being posted on websites, such as racist comments, pornography, terrorist activities and so on.
   ② Some form of control would prevent children and other vulnerable groups being subjected to undesirable websites.

   Asma was against the argument and put forward two of her own reasons.
   ① Material published on websites is already available from other sources.
   ② Policing would go against freedom of information and freedom of speech.

   Put forward your own arguments and discuss whether you think Mariam's or Asma's reasons are valid.
3 Describe the main differences between the terms: *legal, morality, ethics* and *culture*. Give examples of each.

7.2 Copyright issues

Key terms

Piracy – the practice of using or making illegal copies of, for example, software.

Product key – security method used in software to protect against illegal copies or use.

Digital rights management (DRM) – used to control the access to copyrighted material.

Free Software Foundation – organisation promoting the free distribution of software, giving users the freedom to run, copy, change or adapt the coding as needed.

Open Source Initiative – organisation offering the same freedoms as the Free Software Foundation, but with more of a focus on the practical consequences of the four shared rules, such as more collaborative software development.

Freeware – software that can be downloaded free of charge; however, it is covered by the usual copyright laws and cannot be modified; nor can the code be used for another purpose.

Shareware – software that is free of charge initially (free trial period). The full version of the software can only be downloaded once the full fee for the software has been paid.

7.2.1 Software copyright and privacy

Software is protected by copyright laws in much the same way as music CDs, videos and articles from magazines and books are protected.

When software is purchased, there are certain rules that must be obeyed:
- It is illegal to make a software copy and sell it or give it away.
- Software cannot be used on a network or used on multiple computers without a multi-use licence.
- It is illegal to use coding from copyrighted software in your own software – and then pass this software on or sell it as your own – without the permission of the copyright holder.
- It is illegal to rent out a software package without permission to do so.
- It is illegal to use the name of copyrighted software on other software without agreement to do so.

Software **piracy** (making illegal copies of software) is a major issue among software companies. They take many steps to stop the illegal copying of software and to stop illegal copies being used once they have been sold:
- When software is being installed, the user will be asked to key in a unique reference number or **product key** (a string of letters and numbers) which was supplied with the original copy of the software (for example: 4a3c 0efa 65ab a81e).
- The user will be asked to click a button or box which states they agree to the licence agreement before the software continues to install.
- The original software packaging often comes with a sticker informing the purchaser that it is illegal to make copies of the software; the label is often in the form of a hologram indicating that this is a genuine copy.
- Some software will only run if the CD-ROM, DVD-ROM or memory stick is actually in the drive; this stops illegal multiple use and network use of the software.
- Some software will only run if a dongle is plugged into one of the USB ports.

(See also Section 7.2.2 regarding further copyright protection using DRM.)

The Federation Against Software Theft (FAST) was set up in the UK to protect the software industry against piracy. FAST prosecutes organisations and individuals involved in any copyright infringements.

Similar organisations exist in other countries. The following extract from a newspaper article describes a typical example of how strict the anti-piracy laws are in some countries.

TRADERS FINED $100 000

Two eBay traders from the United States of America agreed this week to pay a total of $100 000 in damages after they were caught selling illegal copies of Norton security software.

The SIIA settled the case against the two traders who also agreed to stop selling illegal software and provided SIIA with records identifying their customers and suppliers.

7.2.2 The internet and the World Wide Web (WWW)

Digital rights management (DRM) was originally set up to control what devices a CD could play on. Preventing a CD from playing on a computer, for example, would help stop it being copied illegally. DRM has since been updated to cover more areas; it does this by using protection software to help stop the copying of, for example, music tracks, video files or ebooks. DRM creates restrictions that control what the users can do with the data. For example, allowing a music file to be streamed over the internet but not copied, allowing an ebook to be read on a tablet only, or a game requiring an internet connection to a certain website to work, and so on. The aim of DRM is to ensure that any attempt made to break the copyright protection will produce a defective copy which will not work.

When you buy a product protected by DRM, it may come with a key which licences a single user on one device and this key must be registered. Another example – of which there are many – is Apple Music's use of DRM layers in streamed music to prevent a user downloading all the music in the first month of a subscription and then cancelling their subscription.

7.2.3 Software licensing

Commercial software

Commercial software is available to customers for a fee, providing a licence for one genuine copy to be used on a single device, or a multi-use licence for multiple users. Occasionally, software is offered free of charge if an earlier version was bought by the user. This type of software is fully copyright-protected and none of the code can be used without the prior consent of the copyright owner.

Free software and the Open Source Initiative

The **Free Software Foundation** and the **Open Source Initiative** are non-profit organisations that promote the benefits of giving users the freedom to run, copy, change and adapt software. Examples of software licensed in this way include: F-spot (photographic manager), Scribus (DTP/word processor) and LibreOffice (Office Suite). Users are allowed to follow the four freedoms:

- Run the software for any legal purpose they wish.
- Study the program source code and modify it where necessary to meet their needs.
- Redistribute copies of the software to friends and family.
- Distribute code modified by the user to friends and family.

Users do not need to seek permission to do the above since the software is not protected by copyright restrictions. However, there are still some rules that the user must adhere to. Users cannot

- add source code from another piece of software unless this is also described as free software or open source software
- use the source code to produce software which copies existing software which is subject to copyright laws
- adapt the source code in such a way that it infringes copyright laws protecting other software
- use the source code to produce software which is deemed offensive by third parties.

While the two organisations promote the same four freedoms, they have different basic philosophies.

Free Software Foundation focuses on what the recipient of the software is permitted to do with the software.

Open Source Initiative focuses on the practical consequences offered by the four freedoms; the aims are to provide effective collaboration on software development by the users. There are ten principles that have been developed to ensure the philosophy of the Open Source Initiative is adhered to:

1 **Free Redistribution** The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.
2 **Source Code** The program must include source code and must allow distribution in source code as well as compiled form. Where some form of a product is not distributed with source

code there must be a well-publicised means of obtaining the source code for no more than a reasonable reproduction cost, preferably downloading via the internet without charge. The source code must be the preferred form in which a programmer would modify the program. Deliberately obfuscated source code is not allowed. Intermediate forms such as the output of a preprocessor or translator are not allowed.

3 **Derived Works** The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software.

4 **Integrity of The Author's Source Code** The license may restrict source-code from being distributed in modified form only if the license allows the distribution of 'patch files' with the source code for the purpose of modifying the program at build time. The license must explicitly permit distribution of software built from modified source code. The license may require derived works to carry a different name or version number from the original software.

5 **No Discrimination Against Persons or Groups** The license must not discriminate against any person or group of persons.

6 **No Discrimination Against Fields of Endeavor** The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

7 **Distribution of License** The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.

8 **License Must Not Be Specific to a Product** The rights attached to the program must not depend on the program's being part of a particular software distribution. If the program is extracted from that distribution and used or distributed within the terms of the program's license, all parties to whom the program is redistributed should have the same rights as those that are granted in conjunction with the original software distribution.

9 **License Must Not Restrict Other Software** The license must not place restrictions on other software that is distributed along with the licensed software. For example, the license must not insist that all other programs distributed on the same medium must be open-source software.

10 **License Must Be Technology-Neutral** No provision of the license may be predicated on any individual technology or style of interface.

Freeware

Freeware is software a user can download from the internet free of charge. Once it has been downloaded, there are no fees associated with using the software (examples include: Adobe Reader, Skype and some media players). Unlike free software, freeware is subject to copyright laws and users are often requested to tick a box to say they understand and agree to the terms and conditions governing the software. This means that a user is not allowed to study or modify the source code in any way.

Shareware

Shareware allows users to try out some software free of charge for a trial period. At the end of the trial period, the author of the software will request that you pay a fee if you wish to continue using it. Once the fee is paid, a user is registered with the originator of the software and free

updates and help are then provided. Often, the trial version of the software is missing some of the features found in the full version, and these do not become available until the fee is paid.

This type of software is protected by copyright laws and users must not use the source code in any of their own software without permission.

ACTIVITY 7B

1 a) What is meant by the term *software piracy*?

   b) Describe **three** ways of protecting software against deliberate attempts at making copies to sell or give away.

2 A software company offers a suite of shareware programs. It contains a spreadsheet, word processor, database and drawing package.
   What are the benefits to the following two stakeholders of offering software packages as shareware?

   • The company

   • The customer

7.3 Artificial intelligence (AI)

Key terms

Artificial intelligence (AI) – machine or application which carries out a task that requires some degree of intelligence when carried out by a human counterpart.

7.3.1 What is AI?

Artificial intelligence (AI) is a machine or application which carries out a task that requires some degree of intelligence when carried out by a human being. These tasks could include

- the use of a language
- carrying out a mathematical calculation or function
- recognising a person's face
- the ability to operate machinery, such as a car, an aeroplane or a train
- analysing data to predict the outcome of a future event, such as weather forecasting.
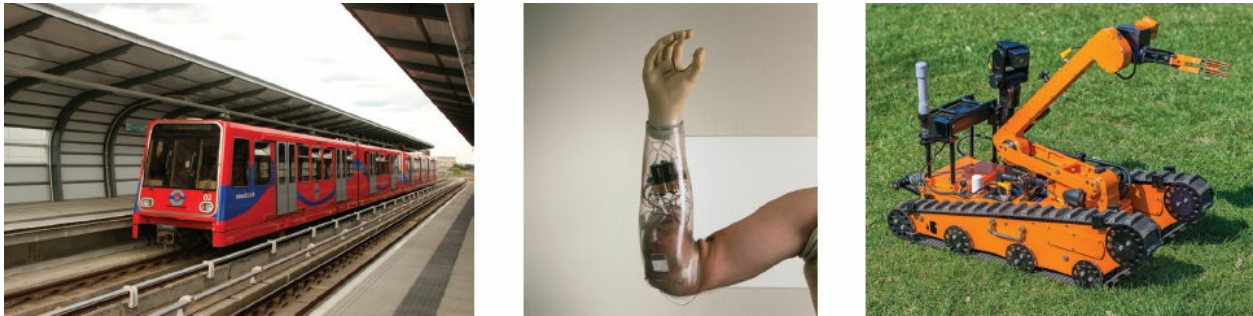

Figure 7.2 Examples of how AI can be used in every-day life

AI duplicates human tasks requiring decision-making and problem-solving skills.

7.3.2 The impact of AI

People often associate AI with science fiction, fantasy and robots. Numerous films and books fuel this association. The science fiction author, Isaac Asimov, went so far as to produce his own three laws of robotics:

1 A robot may not injure a human through action or inaction.

2 A robot must obey orders given by humans without question.

3 A robot must protect itself unless it conflicts with the two laws above.

However, AI goes way beyond robotics. It covers an ever-increasing number of areas, such as
- autonomous (driverless) vehicles
- artificial limb technology
- drones, used to carry out dangerous or unpleasant tasks such as bomb disposal, welding, or entering nuclear disaster areas
- climate change predictions
- medical procedures, such as eye operations where extreme precision is required.

7.3.3 The impacts of AI on society, the economy and the environment

As a result of increasing automation over the next few decades, the human race will need to consider the impacts that AI will have on society, the economy and the environment. So should we all be worried? In this section, we will consider a number of existing AI technologies, plus some predictions for the future, to help stimulate discussions. As mentioned in Section 7.3.2, AI is not just about robots, but covers many areas (this is explored further in Chapter 18, which explores specific AI technologies in more depth).

We will look at some of the areas mentioned in Section 7.3.2 in more depth and consider the implications of using AI (the descriptions that follow will mix up benefits and drawbacks – in Activity 7C you will need to consider the overall impact).

New developments in AI are constantly being announced and you are advised to keep up to date by checking out the many websites that keep an eye on AI development.

Below are some of the developments and impacts that are currently expected to be seen in the near future.

Research has predicted that, by 2030, some 600 million jobs will be lost globally and as many as 400 million people will need to retrain or switch jobs – all caused by the inevitable advances in AI. The most likely jobs to be lost are those doing medium- and low-skilled work, but high-skilled jobs (such as hospital technicians, architects, engineers) are also at risk. This could lead to civil unrest with large numbers of young people out of work, with few or no employment prospects, unless they have a sought-after skill.

History has shown, however, that previous technological advances all ended up creating a net increase in jobs. As automation takes over, jobs on the factory floor are lost, but production becomes much faster and more efficient, thus requiring an increase in the number people doing tasks that the automation process cannot yet do, such as quality control, test driving new vehicles and so on. Technology creates new jobs which are generally more interesting to humans than the manual jobs which are lost. However, history does not always repeat itself, so we need to prepare ourselves for a large reduction in employment and think about how to redistribute wealth so that the overall impact of AI will be positive.

It is predicted that, eventually, 99% of all jobs could be eliminated since the increase in the use of AI is exponential – competition between countries and companies to expand their economies will continue to fuel this growth. One question that might be legitimately asked is, 'if 99% of jobs disappear, who will build the robots and maintain them?' To answer that question, let us consider a present-day solution to the question. 3D printers are actually now being designed and made by other 3D printers with no human interaction – the whole process is automatic with AI algorithms in control of the building, design and maintenance of these printers. So, it seems logical that other robots/machines will build and maintain future robots and other AI systems.

An increase in AI will leave people with more time to pursue their hobbies and have a better lifestyle. Previous industrial revolutions have led to steep changes in the economies of countries that embrace the new technology. Being left behind is not an economic option but is it a good environmental option?

Improvements in AI technology can have a positive impact on the environment. Scientists now have more information than ever about what affects the environment. AI can help by finding patterns and interconnections within the thousands of data sets. This helps scientists make informed predictions about the environment and potential climate change. Since this analysis is very complex, the use of AI systems can speed up this process incredibly and allow the human race to take action much faster than they could by present methods. Here are some potential ways in which AI can help:

- AI can help us to conserve natural resources (for example, improve the conservation of water supplies).
- Detection of pollution in the air and in the seas using AI is much more accurate, allowing scientists to pinpoint the source(s) of pollution more accurately and much faster.
- In the future it could be possible to combine weather forecasting and AI to allow for better predictions about renewable energy resources needed for the next few days. This would lead to a more precise automated renewable energy forecast using solar, tide, thermal and wind energy generation.
- AI would allow us to learn from nature's ecosystems by monitoring and modelling, for example, a river's ecosystem. This would enable us to gain a better understanding of what can affect the delicate balance of life in the river. Such real-time environmental monitoring would allow us to quickly take remedial action before the affects became irreversible. AI would make this possible due to the ability to analyse vast amounts of very complex (inter-related) data.

We will now look at three particular areas where AI could have a large impact.

Transport

Some taxi companies are already looking at the introduction of autonomous (driverless) cars. A customer can call up the taxi using an app on their mobile phone, which also automatically handles the payment. Information about the taxi (such as its location and estimated arrival time) would be sent to the mobile phone until the driverless taxi arrives at the exact pick-up point. There would not be any people anywhere in the chain, with AI systems taking total control. Some car manufacturers are on the brink of actually supplying autonomous vehicles (cars, buses and trucks). This would be much more efficient but would put many drivers out of a job.

Criminal justice system

Advances in facial recognition systems is making fingerprinting in forensic science almost obsolete. AI is also being used to automate legal work and some courts in the USA have trialled the use of AI to sentence criminals and even decide if a prisoner is eligible for parole. Is this a bad thing? Here are some questions to think about:

- Does government use of AI need a warrant to allow online data to be searched for all potential criminal activity?
- Can AI be used to listen in to our mobile phone conversations and assess our emails? Social media companies are already coming under pressure in this area – would AI help this or could criminals make use of it to hide criminal activity?
- What about legal malpractice – what would be the mechanism to challenge an AI inspired legal decision?
- How do we ensure no bias creeps into AI decision making processes? The software being

trialled in the USA to determine a prisoner's suitability for parole is already showing bias against black African Americans. How do we ensure such prejudices by governments and individuals when using AI systems is not allowed to occur?

Advertising and use of data

You may remember the Cambridge Analytica scandal in 2018 which hinged around potential misuse of data obtained from a social media company (nearly 90 million profiles had been used by the company leading some people to believe it had influenced the 2016 USA presidential elections). AI could reduce such occurrences by allowing much closer monitoring. It would need to be very sophisticated and act quickly to have any real impact – human beings certainly could not respond fast enough.

Algorithms can now tailor advertising aimed at specific people by using AI machine learning – this is done by building personality profiles of every internet and mobile phone user. Data is picked up from search engines, social media and visits to websites – all this data can be analysed by machine learning algorithms (see Chapter 18 for more details).

ACTIVITY 7C

Look through this chapter on the impacts of AI and produce a short essay or wall display highlighting the pros and cons. Draw a reasoned conclusion and debate the overall impact of AI with your classmates.

ACTIVITY 7D

1 In 2017, Diane Bryant, the chief operating officer of Google Cloud, claimed that AI can:
   • help us manage the Earth's very scarce resources
   • improve cancer diagnosis using precision medicine leading to customised treatments
   • lead to improvements in human rights in many countries due to cloud computing, better connectivity and reduced costs in developing faster computers.

   Describe, with examples, why Ms Bryant's claims could help people in the future.
2 Give **three** different examples of AI.
   For each of your examples, give **one** benefit and **one** drawback to the general public.

End of chapter questions

1 Nicolae has joined a software company as a new team manager. During his induction he was given a presentation on the company's code of conduct and the company's expected ethical behaviour.
   He was given hand-outs after the presentation which included the code of conduct and ethical behaviour.
   a) Explain what is meant by the term *611*.

   [2]

   b) Describe the differences between behaving in an unethical manner and in an illegal manner.

c) Nicolae joins a team writing new software in a programming language unfamiliar to him. Part of his job will be to visit a client and oversee the team writing the software to meet the client's requirements.

He has little previous experience of working off-site at the client's premises, and has to depend on a junior colleague to help him through the process. This makes Nicolae uncomfortable in his role as project manager.

After six months with the company, Nicolae will have a meeting with his own line manager. The line manager will check Nicolae's progress against the IEEE eight principles and code of practice. Nicolae has decided to raise three issues with his line manager.

i) Describe **three** issues he could legitimately raise.

[3]

ii) State which of the IEEE's eight principles each issue described in part c) i) comes under.

[3]

iii) Describe what actions the line manager should take to address the three issues you raised in part c) i).

[3]

2 a) Name **three** types of software licensing.

[3]

b) For each example, describe **three** features which identify the differences between them.

[3]

c) Describe how copyright issues affect each type of named software licensing.

[3]

3 a) Computers over the years have been described as first to fifth generation. Identify the generation that is associated with AI.

[1]

A first
B second
C third
D fourth
E fifth

b) AI is involved in problem-solving. Identify the term that is used to describe the 'common sense' part of problem-solving.

[1]

A analysis
B critical design
C heuristics
D programming
E sampling

c) Identify the statement that best describes AI.

[1]

    A inputting knowledge into a computer

    B programming a computer using an expert's experiences

    C playing a strategic game, such as chess

    D making a machine behave in an intelligent way

    E using a computer to mimic human behaviour

d) Identify the AI process that involves repetition, evaluation and then refinement.
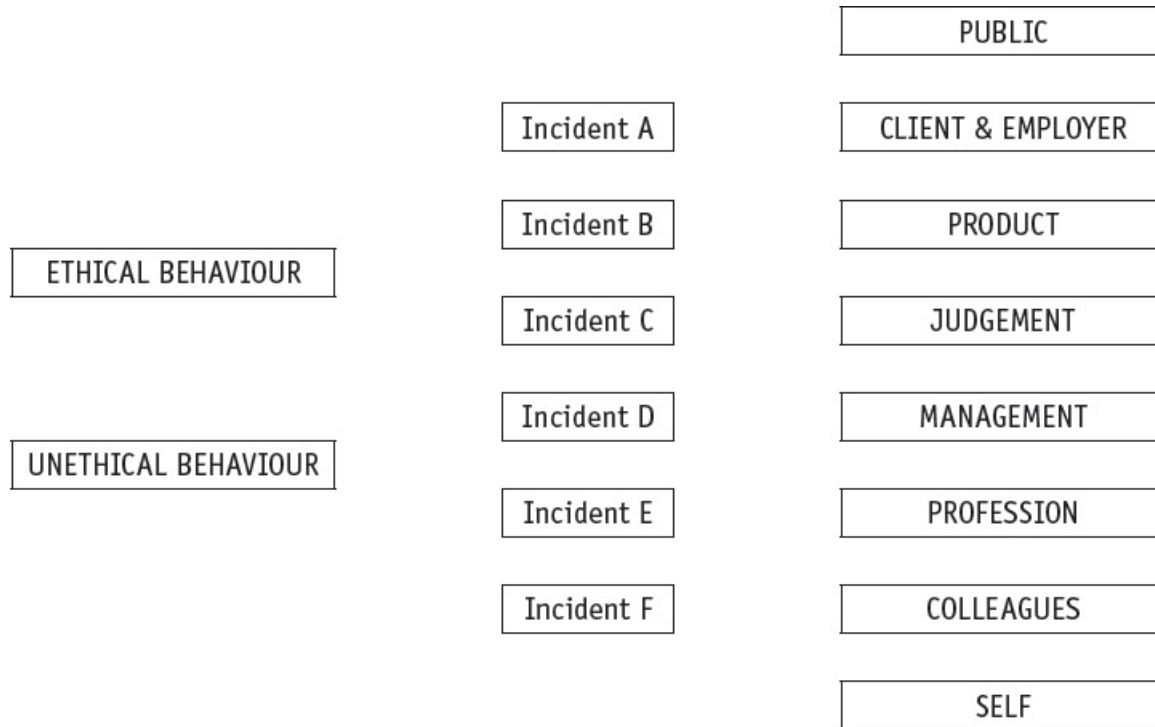
[1]

    A diagnostics

    B fact finding

    C heuristics

    D interpretation

    E iteration

4 The IEEE Software Engineering Code of Ethics uses eight key principles shown in the right-hand column of the following diagram.

Tom is employed as a tester with a software company. He is keen to become a trainee programmer.

The middle column in the diagram labels six incidents which have happened to Tom this week. The table that follows the diagram describes each incident.

		PUBLIC
	Incident A	CLIENT & EMPLOYER
	Incident B	PRODUCT
ETHICAL BEHAVIOUR	Incident C	JUDGEMENT
	Incident D	MANAGEMENT
UNETHICAL BEHAVIOUR	Incident E	PROFESSION
	Incident F	COLLEAGUES
		SELF

Incident	Description

A	Tom has received some phishing emails. He reported this to the bank they were supposed to come from.
B	Tom has asked his manager if they will pay for him to attend a programming course.
C	Tom is testing beta versions of new games software at work. He copies the software on to CD-Rs and sells them to his friends.
D	Tom has completed the application forms to join the Chartered Institute for IT.
E	Tom finds it difficult to work with one of his colleagues. His way of dealing with this has been to refuse to speak with the colleague.
F	Tom's manager had considered the testing of a new game was completed. Tom reported to his manager that he thought there were still bugs which needed to be rectified.

a) Copy the diagram above and connect each of the six incidents to either ethical behaviour or unethical behaviour.

[2]

b) Consider each incident you have identified as **ethical behaviour**.
Indicate the IEE category each incident maps to.

[4]

Adapted from Cambridge International AS & A Level Computer Science 9608 Paper 12
Q5 November 2017