# Answers

**Task 1**

1. Describe, with examples, the **three** major areas that the Computer Misuse Act deals with.

Unauthorised access to computer material - accessing someone else’s computer/data without permission; using someone’s password to log in to a computer and then looking at their files.

Unauthorised access with intent to commit further offences – For blackmail/revenge; phishing for log in details and then stealing money from a bank account.

Unauthorised modification of computer material – knowingly sending a virus to someone; accessing a company’s computer system and altering how the programs work – e.g. hacking into Facebook’s computer systems and then altering how their software works.
2. Describe **three** extra powers that the Police and Justice Act 2006 (Computer Misuse) has added.

Unauthorised access to a computer system was increased from six months to two years in prison.

Making/owning/distributing hacking tools was made illegal (if it is intended to be used for computer misuse.

DoS/DDoS attacks made illegal (with up to 10 years in jail).

See <http://www.legislation.gov.uk/ukpga/2006/48/section/36> for the Police and Justtice
Act 2006

**Task 2**

Look at the following website: <https://www.gov.uk/personal-data-my-employer-can-keep-about-me>

1. Write down **three** items of data which a company can store about an employee.
* name
* address
* date of birth
* sex
* education and qualifications
* work experience
* National Insurance number
* tax code
* emergency contact details
* employment history with the organisation
* employment terms and conditions (eg pay, hours of work, holidays, benefits, absence)
* any accidents connected with work
* any training taken
* any disciplinary action
1. Give **three** moreexamples of data that an employer can only store if they first get the employee’s permission.
* race and ethnicity
* religion
* political membership or opinions
* trade union membership
* genetics
* biometrics, for example if your fingerprints are used for identification
* health and medical conditions
* sexual history or orientation

**Task 3**

* 1. What are the meanings of copyright infringement and plagiarism?

Copyright infringement: is copying something without permission. Copyright infringement is also known as software, video, or music piracy

Plagiarism: is trying to pass off someone else’s idea or work (writing, audio, video) as your own. You may have their permission to use the work, but it is the lack of acknowledgement which makes it plagiarism

* 1. Using the websites below for help, give **one** example of copyright infringement and **one** example of plagiarism.

	**Copyright infringement:**
	Downloading software which hasn’t been paid for / you don’t have a valid licence to use.

	Copying images from a website (without permission) to use in a company brochure.

	Copying a film and giving to a friend to watch; copying music onto someone else’s audio player without permission or payment to the copyright holder.

	**Plagiarism:**
	Obtaining the answers to a homework from a friend and then submitting them as your own work.

	Paying someone to complete an essay for you then submitting as your own work.

	Copying and pasting information from a website into your own work and not referencing where the work came from.

	**See**  <https://www.comfort.txed.net/apps/pages/index.jsp?uREC_ID=336105&type=d&pREC_ID=743676>

	<https://www.thetimes.co.uk/article/cheat-software-spots-essays-students-bought-wk27bnlfs>
* What are **two** consequences of copyright infringement and software piracy?

Economic losses due to copying and piracy are enormous. Artists and creators lose income, governments lose tax revenues and all consumers eventually get less variety and choice.

Companies may go out of business if they cannot prevent copyrighted materials being copied illegally / copyright infringment.

Prices rise for those who do pay to compensate for those who do not.

* Give **three** possible consequences for individuals when using pirated software.

Fines of imprisonment

The software may contain viruses, trojan horses or other malware

The software may damage a user’s disk or other software or operating system

Product documentation may be missing

No warranty or technical support will be provided

Software upgrades and security fixes will not be provided.

**Task 4**

Listed below are some of the laws relating to the IT systems.

* 1. Computer Misuse Act 1990
	2. Police and Justice Act 2006 (Computer Misuse)
	3. Copyright, Designs and Patents Act 1988
	4. Copyright (Computer Programs) Regulations 1992
	5. The Health and Safety (Display Screen Equipment) Regulations 1992
	6. Data Protection Act 2018
	7. Consumer Rights Act 2015

Insert a number in the first column of each row to match each of the statements with one of the above Acts.

One of statements is incorrect and not illegal. For this statement, write ‘Not illegal’.

|  |  |
| --- | --- |
| **Act number**  | **Clause** |
| 4 | With some exceptions, it is illegal to use unlicensed software |
| 7 | Any product, digital or otherwise, must be fit for the purpose it is supplied for |
| 1 | Unauthorised modification of computer material is illegal |
| Not illegal | It is illegal to create or use a hacking tool for penetration testing |
| 6 | Personal data may only be used for specified, explicit purposes |
| 5 | Employers must provide their computer users with adequate health and safety training for any workstation they work at |
| 2 | It is illegal to distribute hacking tools for criminal purposes |
| 3 | It is illegal to distribute an illicit recording |
| 6 | Personal data may not be kept longer than necessary |
| 1 | Gaining unauthorised access to a computer system is illegal |
| 5 | Employers must ensure that employees take regular and adequate breaks from looking at their screens |
| 2 | It is illegal to prevent or hinder access (e.g. by a denial of service attack) to any program or data held in any computer |
| 6 | Personal data must be accurate and where necessary kept up to date |

It is not illegal to create or use a hacking tool **if it is for a legitimate purpose**. “White Hat” hackers use such tools to detect weaknesses in a computer system’s security so that they can be fixed. It is important to note, that the Police and Justice Act (Computer Misuse) (2006) makes it illegal to create, use or distribute hacking tools if they are to be used for malicious purposes.