



Computing GCSE – 1.8

J276/01 – Ethical, Legal, Cultural & Environmental

KEY VOCABULARY

Ethical	Relates to <i>right and wrong</i> but in a moral sense than a legal issue. For example, there is nothing to stop you legally from using Facebook to stalk an ex-partner, but whether it is <i>right</i> to do so, is an ethical issue
Legal	There are certain laws set by government that control how computers can be used – see box
Cultural	These issues relate to society and how technology can affect religious, or social ideas. If people spend all their time on their phones rather than talking face to face, this is a cultural issue
Environmental	How computing impacts on the global and local environments. This might be waste production, or mining to gather resources needed to make phones, or using renewable energy to charge phones, or recycling projects. Companies want to be seen to be 'green'.
Privacy	Privacy is a very important issue. A persons right to privacy is very important and there are strong law, alongside ethical guidance that govern how companies can use our data
Stakeholder	Anyone that is impacted on, in any way, by a technology. They have a vested interest
Open source	Software that is created and shared with the source-code able to be seen. Users are free to make alterations to the source-code to meet their own needs, or to improve the system for everyone
Proprietary	Software that is created but the source code is locked. This is often sold and the company wants to protect its intellectual copyright
Legislation	Laws that relate to a certain area

COMPUTING LEGISLATION

The Data Protection Act (1998)	Sets out how data users who store data about individuals must use that data. It is a set of 8 principles which say how personal data must be collected, used and destroyed. See back of sheet
Computer Misuse Act (1990)	Introduced to deal with the increase in computer hacking in the late 1980s when home PCs started to become popular. It aims to protect computer users against willful attacks and theft of information. The Act makes it illegal to: <ul style="list-style-type: none"> • gain unauthorized access to another person's data • ...with the intention of breaking the law further •to delete, alter or sabotage by introducing viruses
Copyright and Design Patents Act (1988)	Provides the creators of intellectual property (ideas = IP) with proof of ownership, and the exclusive rights to use that idea, and distribute their work. It makes it illegal to copy, modify or distribute IP without permission
Freedom of Information Act (2000)	FOI requires public organisations to publish certain data so the public can access it. It also give individuals the right to request to see all data from over 100,000 public bodies. The act covers all electronic information, such as word docs, emails, digital records. Organisations can withhold certain information if releasing it would affect national security
Creative Commons Licensing	Creative Commons Licensing (CC) is a way that copyright holders can grant certain privileges to publicly use, share, adapt, alter and redistribute IP without written permission.

OPEN SOURCE vs PROPRIETARY SOFTWARE

Open source software is freely available so others can use it. Users can access and modify the source-code and create their own versions.	Proprietary software is not freely available. The compiled code is secured and user must use the software as provided. Any attempt to modify, copy or redistribute the software is a breach of Copyright.
EXAMPLES: Linux, Firefox, Android OS	EXAMPLES: Microsoft Office, Adobe Photoshop, OSX

Data Protection Act (1998)



What are the eight principles of it?

1. Data must be kept secure;
2. Data stored must be relevant;
3. Data stored must be kept no longer than necessary;
4. Data stored must be kept accurate and up-to-date;
5. Data must be obtained and processed lawfully;
6. Data must be processed within the data subject rights;
7. Data must be obtained and specified for lawful purposes;
8. Data must not be transferred to countries without adequate data protection laws.

TYPES OF HACKER



Black Hat – The Bad Guys. They break into systems to cause chaos and steal data for their own benefits

White Hat – Penetration Testing professionals. Often employed by companies to test systems and provide feedback on security

Grey Hat – Not trying to cause damage, but aren't trying to help either.

Red Hat – Scary people – stop Black Hat hackers by revenge hacking and destroying the hacker's system

Green Hat – n00bz trying to learn hacking. Often just download scripts from the internet and run them without understanding the code. Often exploited by Black Hat hackers to do stupid things



Attribution

Others can copy, distribute, display, perform and remix your work if they credit your name as requested by you

BY



No Derivative Works

Others can only copy, distribute, display or perform verbatim copies of your work

ND



Share Alike

Others can distribute your work only under a license identical to the one you have chosen for your work

SA



Non-Commercial

Others can copy, distribute, display, perform or remix your work but for non-commercial purposes only.

NC

