Computing –Privacy and Surveillance

How could data be lost? What could criminals use the data for?

Hacking Accidental deletion Overwriting of files Power cuts Spilled liquids Hard drive worn out Natural disaster e.g. weather Fire	Blackmail Steal identities Make online purchases

Category	Explanation
Legal	Technology provides opportunities to criminals. To help protect people, their data, and their work, several laws have been introduced in the UK.
Environmental	The effect that technology has on the world around us
Cultural	How have society and the ways that we interact been impacted?
Ethical	Considerations about right and wrong, morality and power
Privacy	Once data is put on a computer, it can be easily copied or shared. In some cases, people have a right to choice in this matter.

Computers and the Law

Data Protection Act (DPA) 2018

Computer Misuse Act 1990

Copyright, Designs and Patents Act 1988

Freedom of Information Act 2000

Data Protection Act

Purpose: To control the way that data is handled and to give legal rights to people who have information stored about them.

Who is it for?: We are all “data subjects”. That just means that we have data stored about us and have the right to have the data looked after properly and have the right to see that data. This is called the ‘right of subject access’.

Who makes sure that companies stick to DPA? **Data Controller (DC) and Information Commissioner’s Office (ICO)**

The DC is the person who is responsible for ensuring that the organisation stays within the principles of the Data Protection Act.

The ICO makes sure that the companies keep to the rules, and fines those that don’t, sometimes heavily.

The principles of the Data Protection Act 2018

1. Personal data must be fairly and lawfully processed
2. Personal data must be obtained for specified, explicit and legitimate purposes
3. Personal data muse be adequate, relevant and not excessive
4. Personal data must be accurate and up-to-date
5. Personal data must not be kept longer than necessary
6. Personal data must be handled in a way that ensures security

Computing –Privacy and Surveillance

Stakeholder

Stakeholders are groups or individuals who will be affected by or can change the way the technology is used.

Right to be forgotten

The right to be forgotten (part of GDPR) means that an individual can request that an organisation erases all their personal data. This right only applies in certain circumstances, e.g. the personal data is no longer necessary for the purpose for which an organisation originally collected or processed it.

Copyright, Designs and Patents Act 1988

The Copyright, Designs and Patents Act 1988 exists to protect people's creations. When a person creates something, they own it. E.g.

A picture, photograph, recording of music, television programme, film, text (book, article or report), algorithm (but only once the source code has been created)

When is it legal to copy, publish, distribute, or sell copyrighted material?

- When you are the copyright holder
- When you have the copyright holder's permission
- When the copyright holder has chosen to give up their copyright

Open Source V's Proprietary Software

Proprietary software cannot be copied/altered (without permission of the copyright owner)

Open source software can be modified (provided it remains open source)

Proprietary software is distributed only as a completed program; the source code is not available

Open source software is distributed with its source code

Creative Commons (CC)

A creative commons licence is one of several public copyright licenses that enable the free distribution of an otherwise copyrighted work.

The work must not be used for commercial purposes and should not be changed

Use appropriately licensed material.

Legal use of other people's work

Credit the creators of the material.

Credit the source/website of the material.

Freedom of Information Act 2000

The Freedom of Information Act was introduced to give **any** member of the public the right to access any information recorded by public sector organisations. These organisations include: Schools, councils, government departments, health trusts and hospitals, libraries and museums.
Requests must be made in writing, either by letter or by email. The organisation then has 20 working days to provide the information.

When doesn't the organisation have to respond?

It would cost too much or take too much staff time to deal with the request
The request is vexatious (designed to create annoyance)
The request repeats a previous request from the same person
In addition, requests cannot be responded to if they contravene data protection or GDPR

Why is the Freedom of Information Act important? It promotes social justice. 'Social justice' refers to creating an equal society where everyone is treated fairly and has equal opportunities. Public organisations act on everyone's behalf and spend money that belongs to everyone; therefore, everyone has a right to know how that organisation operates, and what they spend public funds on.

Computing –Privacy and Surveillance

Computer Misuse Act 1990

The Computer Misuse Act (1990) and its amendments were created so that unauthorised access to computers and crimes committed using a computer could be prosecuted. The act is

PRINCIPLES	LEGAL ACTIONS
Unauthorised access to digital/computer material. This means a person asking a computer to perform any function with the intent of accessing anything on the computer for which they do not have permission, and for which they know they do not have permission.	Punishable by up to two years in prison and a £5,000 fine.
Unauthorised access to digital/computer material with intent to commit or facilitate the commission of further offences. This means a person gaining access to a computer without permission in order to commit another crime or to enable someone else to commit a crime.	Punishable by up to five years in prison and an unlimited fine determined by the damage caused and the severity of the crime.
Unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of a computer. This means a person intentionally impairing the operation of any computer or program, or intentionally preventing access to any data or program on any computer. This includes creating or supplying materials that could be used to carry out this offence.	Punishable by a prison sentence of up to ten years and an unlimited fine, but if the act puts life at risk or endangers national security, the sentence may be extended to life imprisonment.

Cultural impact of technology

'Culture' means 'relating to the ideas, customs, and social behaviour of a society', i.e. 'how we do things around here'. 'Impact' means 'to have an effect on something'.

- Impact on daily lives
- Digital Divide
- Globalisation

E-Waste

Use of non-recyclable materials, Depletion of rare chemical elements,
Harmful effect of pollution caused by disposal and recycling to environment and health of recyclers through exposure to toxins.

Downtime

'Downtime' describes situations where an organisation loses some or all of its IT systems for a period of time. This could be for any number of accidental or deliberate reasons, including:

- Planned maintenance and system upgrades
- Power or ISP failure
- Cyberattacks
- Human error
- Natural disasters

Artificial Intelligence (AI)

Artificial intelligence is technology that enables a computer to think or act in a more 'human' way.

Algorithm

An algorithm is a set of instructions that describes how to get something done.

The Digital Divide

The digital divide is the division that exists between people who have access to and can use technology, and people who don't have access or cannot use it:

People who live in rural areas-Slower internet speeds, delayed access to repairs

People who live in developing countries

People in low-income households

People with poor computer skills

Elderly people

Some people who have disabilities

The Investigatory Powers Act 2016

This act sets out rules on the use of investigatory powers by the police and security and intelligence agencies. Phone companies and internet service providers are required to keep copies of users' emails and browsing histories for 12 months. It also gives the police and security services the authority to access computers and phones to search for data.