General Principals

- In many cases there is no right or wrong answer and many people have differing viewpoints.
- It is important to be aware of different views and concerns and to be able to discuss them.
- In general people value privacy and do not like governments, security services or companies to have too much access to their data.
- Governments often argue that they need this data to protect people, prevent terrorism and maintain security.
- Companies often argue they need access to data to monitor and improve services.
- Digital Divide is a term referring to a divide in society between those with access to technologies and those without it.

Cyber Security, Hacking and Unauthorised Access

- Discussed in more detail in Topic 6.
- Most countries have laws against hacking and unauthorised access to systems.
- The theft of computer equipment is covered by conventional legislation.
- Data protection laws require companies to keep data hold secure.

Issues

- How can we prove someone deliberately hacked a system?
- Hackers may post people's information online, impacting privacy.
- How can laws keep up as technology evolves?

Wearable Technologies

- Technology such as smart watches, smart glasses and other fitness devices which are worn on the body.
- The most known example is the fit bit.
- May collect data about the wearer.
- May allow the wearer to easily access data and control devices.

Issues

- What happens to data collected by these devices?
- How secure is the communication between these devices?
- Is there a risk of a "digital divide" between those who can and cannot afford these devices?
- These devices are inconspicuous , making them

Cloud Storage

- Discussed in more detail in topic 3.
- The storage of files and data at a location which is accessed via The Internet.

Issues

- How secure is the communication with cloud storage?
- Data is subject to different laws based on where it is stored.
- Laws may require organisations to store data in certain countries.
- The data centres used for cloud storage require huge amounts of power to run and cool servers, where does this power come from? What are the environmental implications of generating it?
- How private is data stored in the cloud? Can the provider's employees access it?
- Should governments be allowed to access data stored in the cloud to prevent crime?

Topic 8: Ethical, Legal and Environmental Impacts of Digital Technology on Wider Society

Wireless Networking

- Wireless networks are more and more common.
- Many businesses offer free wireless Internet access to people using their services.

Issues

- How secure is the communication between devices?
- Should governments be able to intercept communications to maintain security and prevent terrorism?
- Some people have concerns about the health impacts of wireless networks.
- Is there a risk of a "digital divide" forming between those with access to fast wireless networks and those without it.
- Data sent on public wireless can often be easily intercepted.
- Who's responsibility is it to keep data secure? The person using the network or the person who operates it?
- How can we track who is using public wireless networks if they use them to commit a crime such as hacking or exchanging illegal material?
- Governments or the providers of the networks may look at the data of those using the network. Is this legal and ethical?

Autonomous Vehicles

- Self driving cars are developing at a rapid pace.
- They use cameras, computers and sensors to know what is around them and drive accordingly.

Issues

- Who is legally responsible in the case of a crash? The drive, the insurer, or the vehicle manufacturer?
- Should a vehicle swerve onto the pavement to avoid a crash which would kill the driver, but in the process kill a pedestrian?
- Should a vehicle drive to avoid hitting a dog if doing so would cause a crash which might injure the driver?
- How can the batteries and other components be manufactured and disposed of without damaging the environment?
- Are these vehicles legal to use?
- Is it ethical for governments to access the cameras on vehicles to detect crime?
- How can the data collected, such as car's location, be kept private?

Mobile Technologies

- Mobile phones, tablets and other mobile technologies continue to rapidly evolve.
- Devices are getting smaller and more powerful.

Issues

- Is there a risk of a "digital divide" between those who can and cannot afford these devices?
- Some services may need a phone number of smartphone app to access. What about those who do not have, want or know how to use these devices?
- Devices change rapidly, causing excess waste which can be harmful to the environment.
- Devices are often hard to repair, and so are replaced rather than repaired.
- Should governments be able to intercept communications to maintain security and prevent terrorism?

Computer Based Implants

- Technology or other electronics implanted into the human body.
- Often used to assist those with a disability such as a bionic eye.
- GPS tracking chips can be implanted into people.

Issues

- Is it ethical to implant electronics into people?
- How secure is the communication between these devices?
- Is there a risk that those who cannot afford this may loose out?
- How can the data collected be kept safe and secure?
- The data from these devices is processed by different companies, apps and devices. How is it kept private?
- Who owns the data collected?
- Should governments have access to data collected to monitor their citizens health?
- As these devices are relatively new, the long term health risks are often not known.