FACTFILE:
GCE PROFESSIONAL BUSINESS SERVICES

UNIT A2 1: SOCIAL, MORAL AND ETHICAL ISSUES

Rewarding Learning

Learning Outcomes

Student should be able to:

Students should be able to analyse the social, moral and ethical issues for a business using technology, including:

- automated decision making;
- online censorship;
- monitoring personal behaviour;
- capturing, storing and analysing personal information;
- the digital divide; and
- acceptable use policy.

Background and Definitions

Businesses are making increased use of technology to improve efficiency in the delivery of products and services. The use of technology in business has led to a range of issues mainly around how this might infringe on individual rights. For example, issues related to the above bulleted points include:

- Consequences of using automated decision making technology and equality.
- Online censorship and the right to freedom of expression.
- Monitoring personal behaviour and the right to privacy.
- Capturing, storing and analysing personal information and privacy.
- The digital divide, access and use of technology and equality of opportunity.

These issues can be considered as **social issues**. Social issues are those which affect peoples' lives. The above issues can also be viewed from **moral** and **ethical** perspectives and therefore as **moral** or **ethical** issues. Moral or ethical issues are typically controversial and involve making decisions about what is right and wrong or good and bad.

- **Moral** - an individual's sense of what is right and wrong. Morality is concerned with an individual's behaviour rather than the character or the values of the person who performs the actions.
- **Morals** - an individual's principles guiding a person's sense of right and wrong.
- **Ethics** - the basic principles or rules of conduct guiding individual and group actions and behaviour based on social norms and values. Ethics define our morals and help people to distinguish what is right from wrong.

In the case of the above examples businesses have to make policy and operational decisions based on balancing moral and ethical considerations with meeting business needs and in accordance with

legislation and regulations such as General Data Protection Regulations (2018) and Human Rights laws. One of the ways businesses can do this is to develop and implement an acceptable use policy.

AUTOMATED DECISION MAKING TECHNOLOGY

Automated decision making technology is technology which is used to make decisions. This involves programmed technology reading or profiling data about individuals, evaluating specific fields of information against criteria and making decisions based on this. Automated decision making technology is being used to make decisions in the following areas:

- Criminal Justice System.
- Education.
- Financial Services.
- Health care.
- Social Media Advertising.

Moral and ethical Issues arise because automated decisions affect people's lives and wider society and in the worst cases can have serious consequences.

Example

2018 England – NHS breast screening programme, since 2009 450,000 women aged between 68 - 71 were not invited for a final screening appointment, affecting women currently up to the age of 79. It was estimated that around 100-300 women may have had their lives shortened as a result.

https://breastcancernow.org/news-and-blogs/blogs/the-breast-screening-programme-failure

It is the parameters of analysis that are applied to the input data that can lead to anomalies and discrimination. The decision making process can be flawed or discriminatory if the parameters used are based on inaccurate, incomplete assumptions, poor data sampling and using inappropriate statistical methods.

The individuals responsible for designing the decision making system, setting the parameters for the decision making process and those administering the system have a moral responsibility to ensure the decisions made are fair, reliable and credible and applied consistently over time.

Moral Issues

The behaviour of individuals responsible for the automated decision making system can lead to moral issues around the following:

- confidentiality;
- possible inherent bias;
- fairness in relation to criteria applied and outcomes of decisions;
- impact on the lives of individuals; and
- accepting responsibility for decisions, consequences and outcomes.

Ethical Issues

Ethical Issues can result from how the business uses automated decision making technology. These include:

- consent;
- who has access to the information;
- sharing information with third parties;
- transparency and openness around the decision making process; and
- individual's right to an explanation of what their personal information is being used for and on how decisions are made;

ONLINE CENSORSHIP

Businesses regularly use online methods for internal and external communications.

These may include:

- Email.
- Instant Messaging.
- Telephone and Smartphone.
- Voicemail.
- Document sharing.
- Text.
- Website.
- Web conferencing.
- Conference calls (Voice, Video and Web).
- Social Media.

One of the main issues around business online communication is whether or not the information or content being communicated is considered to be

in accordance with the businesses **Acceptable Use Policy** and not in breach of legislation.

Government Censorship and Legislation

In the UK and other countries legislation is in place to prevent the public communication of information which is regarded to be offensive, obscene, and malicious or incite to violence. This is a form of censorship which applies to individuals and businesses.

Businesses and Self-Censorship

In addition to legislation around using business technology to communicate information most businesses apply a form of self-censorship in their **Acceptable Use Policy.**

Moral Issues

Moral issues can arise when individuals use technology in ways which breach the Business Acceptable Use Policy. These include using technology to download, create, manipulate, store or transmit such as:

- unlawful material, or material that is defamatory, threatening, discriminatory, extremist;
- offensive, obscene or indecent images, data or other material;
- material which promotes discrimination;
- material which breach the privacy of individuals; and
- material which breach intellectual property rights

Ethical Issues

The main ethical issues around censorship concern individual privacy and freedom of speech.

These include:

- criteria applied – In who's interests? Whose criteria? What values are they based on?
- consent;
- application of criteria-fairness and consistency;
- monitoring individual's communications;
- making decisions about and taking action against an employee in breach of acceptable use policy;
- censorship vs business reputation;
- censorship vs public interest; and
- censorship vs risk to public.

MONITORING PERSONAL BEHAVIOUR

Many businesses may monitor employee behaviour for the following reasons:

- security – to protect staff and building and facilities;
- cyber Security – to prevent unauthorised access to computer systems, reduce the risk of hacking, malware, phishing and to protect information;
- compliance – to ensure employees behave in accordance with business policy; and
- performance/productivity – to monitor employees performance and to ensure they are making effective use of their time.

Businesses can use technology to monitor personal behaviour in the following ways:

- closed circuit TV/video;
- telephone monitoring;
- computer monitoring;
- email monitoring; and
- location monitoring/tracking.

Moral issues

The behaviour of individuals with responsibility for monitoring the personal behaviour of others can lead to moral issues:

- decisions about how the information is used depends on the what the person who is monitoring behavior considers inappropriate behaviour – i.e. it involves personal judgement;
- information is used for personal gain e.g. information used for blackmail; and
- surveillance suppressed e.g. video captures an employee behaving inappropriately - not passed on because of the employee's relationship with the individual who is monitoring behavior.

Ethical Issues

- the collection of personal information that is irrelevant to job performance constitutes the basis of privacy violation;
- the personal information gathered may be misused e.g. shared with third parties;
- consent – should businesses monitor employees' behaviour without their consent?

- closed circuit TV/Video monitoring - viewing employee behaviour which is inappropriate or illegal presents an ethical dilemma for the employer – do they take action? If it is illegal behaviour they have a duty to report it to the authorities?
- telephone monitoring - may hear information about employee's personal life e.g. financial problems, medical condition, relationships. The employer has a duty of care, should the employer act on the basis of the conversation?
- computer monitoring/emails – viewing employees' personal email or other communications may disclose employee's personal information to the employer; and
- location monitoring/tracking – informed consent, privacy, right to examine records.

CAPTURING, STORING AND ANALYSING PERSONAL INFORMATION

There are a range of moral and ethical issues around businesses capturing, storing and analysing personal information.

Moral issues (Employees)

The behaviour of individual(s) with responsibility for managing information and the above processes can lead to moral issues where there the individual compromises the privacy and security of the data.

- use of personal information for their own interests/gain;
- data analysis serves personal agenda, the individual deliberately uses the information to present view; and
- does not follow business policy, GDPR requirements and business processes and procedures e.g. does not secure information, leaves personal information in public space.

Moral issues (Customers)

These include:

- providing inaccurate, incomplete, false information e.g. Insurance business – customer may not fully disclose all the information required in order to get a reduced insurance premium.

Ethical Issues

These include:

- transparency;
- consent – individuals should have a right to know and consent to information being
- captured by businesses;
- collect only the information required for business purposes;
- freedom from unauthorised access to private data;
- inappropriate use of data;
- accuracy and completeness when collecting data about a person or persons by technology;
- communication of data breech's to customer and appropriate authorities;
- availability of data content, and the data subject's legal right to access; ownership;
- the right to inspect, update or correct these data; and
- retention and disposal of personal information.

THE DIGITAL DIVIDE

The digital divide is a term used to describe a gap in access and use of digital technology (computers, internet, mobile phones...) between different individuals, different groups, or between different regions or different countries. This leads to inequalities in access to opportunities, knowledge, services and goods.

Reasons for the Digital Divide

- **Geographical Location** – some regions may not have access to internet. People living in those regions may be disadvantaged over others who have internet access. This limits their access to information from a range of online services and social networking sites.
- **Digital Literacy** – People who lack the knowledge and skills to use digital technology are disadvantaged over others who are competent in using technology. People who are competent in using technology will have an advantage when applying for jobs.
- **Income Levels** – access to technology, service provision, hardware and software has financial implications. People with higher levels of income may have more money to spend on digital technology.

ACCEPTABLE USE POLICY

An acceptable use policy is a written document which outlines the acceptable practices and restrictions around the different types of technology the business uses including:

- Email.
- Instant Messaging.
- Telephone and Smartphone.
- Voicemail.
- Document sharing.
- Text.
- Website.
- Web conferencing.
- Conference calls (Voice, Video and Web).
- Social Media.

An acceptable use policy for business technology sets out rules of conduct or ethical principles. These guide individual actions and behaviour when using technology. Ethical principles are based on social norms and values of what is right and wrong.

Before using business technology employees are usually required to read and agree to using technology in the ways described in the acceptable use policy. An acceptable use policy regulates the use of technology in business. This helps to:

- Reduce risk to the business from cyber-attacks.
- Prevent/reduce the irresponsible use of resources.
- Prevent breaches of confidentiality.
- Prevent breaches of privacy laws and regulations.
- Protect the business's reputation.
- Protect the employee's reputation.

An acceptable use policy must balance individual rights and privacy with ensuring that employee understands the risk to themselves and to the business for failure to properly use company resources.