MODULE 8:
IMPACT OF IT ON SOCIETY

Social media and online behaviour. Social media platforms such as Facebook, Twitter and Instagram allow us to connect with people around the world, share our opinions and interests, and access information and entertainment. However, they also pose some challenges and risks, such as cyberbullying, fake news, privacy breaches and addiction. We need to be aware of these issues and use social media responsibly and ethically.

Technology for social good. IT can also be used to address social problems and improve the lives of people in need. For example, IT can help with disaster relief, health care, education, environmental protection and human rights. There are many initiatives and organizations that use IT for social good, such as the United Nations, the Red Cross, Khan Academy and Wikipedia. We should support and participate in these efforts to make a positive difference in the world.

Accessibility and inclusion. IT can also help to reduce barriers and inequalities for people with disabilities, minorities, women and other marginalized groups. For example, IT can provide assistive devices, adaptive software, online learning and remote work opportunities for people with disabilities. IT can also promote diversity, inclusion and empowerment for people from different backgrounds, cultures and perspectives. We should respect and celebrate the diversity of people in the IT field and society at large.

8.1. SOCIAL MEDIA & ONLINE BEHAVIOUR

Social media platforms have become an integral part of our lives, connecting us with people, information and entertainment.

There are significant risks for individuals and organisations, such as cyberattacks, privacy breaches, misinformation and ethical dilemmas. How can we use social media responsibly and safely, while enjoying its benefits?

PROTECT YOUR DATA & DEVICES

One of the main threats of social media is that hackers can exploit the data you share online to launch cyberattacks, steal your identity or access your accounts. To prevent this, you should:

- Use strong passwords and change them regularly.
- Enable two-factor authentication for your accounts.
- Avoid clicking on suspicious links or attachments.
- Update your software and antivirus regularly.
- Review your privacy settings and limit what you share publicly.
- Be careful when using public Wi-Fi or devices.

BE RESPECTFUL & ETHICAL

Another challenge of social media is that it can amplify negative emotions, opinions and behaviours, such as anger, hatred, discrimination and harassment. To avoid this, you should:

- Think before you post or comment.
- Respect the views and feelings of others.
- Avoid spreading rumours or false information.
- Report or block abusive or offensive content.
- Follow the rules and guidelines of each platform.
- Seek help if you experience cyberbullying or distress.

LEARN AND GROW

Social media can also be a valuable source of learning and growth, if used wisely and critically. You can:

- Follow reputable sources of information and news.
- Verify the accuracy and credibility of what you read or watch.
- Seek diverse perspectives and opinions.
- Engage in constructive and respectful dialogue.
- Explore new topics and interests.
- Share your knowledge and skills with others.

Social media is a powerful tool that can have positive or negative impacts on society, depending on how we use it. By following these tips, you can make the most of social media, while protecting yourself and others from its risks.

THE NEED FOR ETHICAL POLICIES

Ethical policies are not only beneficial for individuals and society, but also for IT professionals and organizations. They can help to foster trust, reputation, innovation, and competitiveness in the IT sector. They can also prevent or mitigate legal, financial, and reputational damages that may result from unethical IT practices.

Some examples of ethical policies that can be adopted or implemented in the IT field are:

Data protection and privacy policies. These policies aim to protect the personal data of users and customers from unauthorized access, use, disclosure, or deletion. They also specify the rights and obligations of data subjects and data controllers regarding data collection, processing, storage, and transfer.

Cybersecurity policies. These policies aim to ensure the security and integrity of IT systems and networks from malicious attacks or threats. They also define the roles and responsibilities of IT staff and users regarding cybersecurity measures, such as encryption, authentication, backup, and incident response.

Social responsibility policies. These policies aim to promote the positive social impact of IT and to minimize its negative effects on society and the environment. They also encourage the involvement of IT stakeholders in social issues, such as digital inclusion, education, health care, and sustainability.

Professional ethics policies. These policies aim to uphold the ethical standards and principles of the IT profession. They also provide guidance and codes of conduct for IT professionals regarding their duties, rights, and responsibilities towards their clients, employers, colleagues, and society.

Ethical policies are not static or universal. They need to be updated and adapted to the changing IT landscape and to the diverse cultural and legal contexts. They also need to be communicated and enforced effectively to ensure compliance and accountability. Moreover, they need to be supported by ethical education and awareness programs that foster a culture of ethics among IT stakeholders.

Ethical policies are not a burden or a constraint for IT. They are an opportunity and a necessity for IT to contribute positively to society and to achieve its full potential.

PRIVACY PROTECTION & DATA SHARING

As an IT professional, you have a responsibility to protect the privacy of your clients, customers, and users. Privacy is a fundamental human right, and it is also essential for trust, innovation, and competitiveness in the digital economy. However, privacy protection is not always easy or straightforward, especially when it comes to data sharing. Data sharing can have many benefits, such as improving efficiency, quality, and collaboration, but it can also pose significant risks, such as data breaches, identity theft, and discrimination.

How can you balance the need for data sharing with the respect for privacy?

Know the law. Different countries and regions have different laws and regulations regarding privacy and data protection. You should be aware of the legal requirements and obligations that apply to your data processing activities and comply with them accordingly. For example, if you are dealing with personal data from the European Union, you should follow the General Data Protection Regulation (GDPR), which sets high standards for data protection and gives individuals more rights and control over their data.

Know your data. Before you share any data, you should know what kind of data you have, where it came from, how it was collected, what it is used for, and who has access to it. You should also classify your data according to its sensitivity and value and apply appropriate security measures to protect it. For example, you should encrypt sensitive data such as health records or financial information, and limit access to authorized personnel only.

Know your purpose. You should only share data for a specific and legitimate purpose that is compatible with the original purpose of collection. You should not share data for purposes that are unrelated, incompatible, or harmful to the individuals or groups involved. For example, you should not share customer data with third parties for marketing or advertising purposes without their consent.

Know your partners. You should only share data with trustworthy and reliable partners who have a similar or higher level of privacy protection than you. You should also establish clear and transparent agreements with your partners that specify the terms and conditions of data sharing, such as the purpose, scope, duration, security, and accountability of data processing. You should also monitor and audit your partners' compliance with the agreements and the applicable laws.

Know your limits. You should only share the minimum amount of data that is necessary to achieve the purpose of data sharing. You should also respect the rights and preferences of the individuals or groups whose data you are sharing and give them choices and control over their data. For example, you should inform them about the data sharing activities, obtain their consent when required, allow them to access, correct, or delete their data when possible, and respond to their complaints or requests promptly.

ONLINE HARASSMENT & CYBERBULLYING

Online harassment and cyberbullying are serious issues that affect many people, especially children and adolescents. They can cause emotional, psychological and even physical harm to the victims, as well as damage their reputation and relationships.

ONLINE HARASSMENT & CYBERBULLYING

Online harassment and cyberbullying are forms of bullying that use digital technologies, such as social media, messaging platforms, gaming platforms and mobile phones, to intimidate, humiliate, threaten or harm someone else. They can include:

- Spreading lies, rumours or embarrassing photos or videos about someone online
- Sending or requesting nude or nearly nude images or videos (also known as sexting)
- Excluding someone from online groups or conversations
- Making fun of someone's appearance, identity, beliefs or abilities
- Stalking someone online or offline
- Impersonating someone online or hacking their accounts
- Sending hateful or violent messages or threats

Online harassment and cyberbullying can happen to anyone, but some groups are more vulnerable than others, such as girls, LGBTQ+ youth, ethnic minorities and

people with disabilities. Online harassment and cyberbullying can have negative effects on the victims' mental health, self-esteem, academic performance and social skills. They can also increase the risk of depression, anxiety, loneliness, self-harm and suicide.

PREVENTING HARASSMENT & CYBERBULLYING

The best way to prevent online harassment and cyberbullying is to promote a culture of respect, kindness and empathy online. Here are some tips to help you do that:

- Be aware of what you post online and how it might affect others. Think before you share something that could be hurtful, offensive or inappropriate.
- Respect other people's privacy and boundaries. Do not share personal or private information about someone else without their consent. Do not send or ask for nude or nearly nude images or videos.
- Be a positive role model for others. Use positive language and compliments online. Support those who are being harassed or bullied online. Report any abusive or harmful content or behaviour you see online.
- Educate yourself and others about online safety and digital citizenship. Learn how to protect your personal information, passwords and devices online. Learn how to recognize and avoid scams, phishing and malware. Learn how to use privacy settings and blocking features on different platforms. Learn about your rights and responsibilities online.

COPING WITH HARASSMENT & CYBERBULLYING

If you are experiencing online harassment or cyberbullying, you are not alone and you do not deserve it. Here are some steps you can take to cope with it:

- Do not respond or retaliate to the harasser or bully. This might only make things worse or escalate the situation. Instead, ignore them or block them if possible.
- Save the evidence of the harassment or bullying. Take screenshots or record the messages, posts or comments that are abusive or harmful. This can help you report them later or seek legal action if needed.
- Report the harassment or bullying to the platform where it happened. Most platforms have policies and tools to deal with online abuse and hate speech. You can also report the harasser or bully to their school, employer or authorities if they are breaking the law.
- Seek support from someone you trust. Talk to a friend, family member, teacher, counsellor or helpline about what you are going

through. They can offer you emotional support, advice and resources to help you cope.

- Take care of yourself. Online harassment and cyberbullying can affect your physical and mental health. Try to do things that make you happy and relaxed, such as hobbies, exercise, meditation or music. Avoid drugs and alcohol as they can worsen your mood and health.

8.2. TECHNOLOGY FOR SOCIAL GOOD

ETHICAL INNOVATION & POSITIVE IMPACT

Ethical Innovation & Positive Impact: How to Use Technology for Social Good

How can we ensure that our innovations are aligned with our values and contribute to positive social impact?

DEFINE YOUR PURPOSE AND VISION

Before you start developing or implementing any technology solution, you need to have a clear idea of what problem you are trying to solve, who you are serving, and what impact you want to achieve. This will help you set your goals, measure your progress, and communicate your value proposition to your stakeholders.

ENGAGE WITH YOUR USERS AND BENEFICIARIES

Technology for social good should be designed with and for the people who will use it and benefit from it. You need to understand their needs, preferences, expectations, and feedback. You also need to respect their rights, dignity, privacy, and autonomy. Engaging with your users and beneficiaries will help you create solutions that are relevant, accessible, inclusive, and empowering.

CONSIDER THE BROADER CONTEXT AND IMPLICATIONS

Technology for social good should not operate in isolation, but in relation to the social, cultural, economic, environmental, and political context in which it is deployed. You need to consider how your solution will interact with other systems, actors, and norms. You also need to anticipate the potential positive and negative consequences of your solution, both intended and unintended, and mitigate any risks or harms.

ADOPT ETHICAL PRINCIPLES AND STANDARDS

Technology for social good should be guided by ethical principles and standards that reflect your values and commitments. You need to define what ethical innovation means for you and your organization, and how you will operationalize it in your processes, practices, and policies. You also need to align your solution with the relevant laws, regulations, codes of conduct, and best practices in your field.

EVALUATE YOUR IMPACT AND LEARN FROM YOUR EXPERIENCE

Technology for social good should be continuously monitored and evaluated to assess its impact and effectiveness. You need to collect data and evidence that show how your solution is performing, what outcomes it is producing, and what impact it is having on your users, beneficiaries, and society at large. You also need to learn from your experience, reflect on your successes and failures, and improve your solution accordingly.

THE ESSENCE OF TECHNOLOGY FOR SOCIAL GOOD

Technology needs to be guided by ethical principles, aligned with social values, and informed by evidence-based practices.

TECHNOLOGY FOR SOCIAL GOOD

Technology for social good is the use of technology to address social problems, such as poverty, inequality, health, education, environment, and human rights. Technology for social good can take many forms, such as:

- Digital platforms that connect people, resources, and information across borders and sectors.
- Mobile applications that provide access to essential services, such as health care, education, and banking.
- Data analytics that help measure and improve the impact of social interventions.
- Artificial intelligence that enhances human capabilities and supports decision making.
- Blockchain that enables transparency and accountability in transactions and governance.
- Internet of things that enables smart and sustainable solutions for energy, water, and waste management.

POLICIES GUIDING ETHICAL INNOVATION

It is important to have policies that guide ethical innovation and ensure that it aligns with the values and needs of the people it serves.

ETHICAL FRAMEWORK FOR INNOVATION

One possible ethical framework for innovation is based on the Principles for Digital Development, which are nine guidelines that help integrate best practices into technology-enabled programs. They include:

- **Design with the user**. Involve the user throughout the design process and test the solution in real contexts.
- **Understand the existing ecosystem**. Assess the strengths and weaknesses of the current system and identify potential partners and stakeholders.
- **Design for scale**. Plan for growth and sustainability from the start and consider how to reach more users over time.
- **Build for sustainability**. Secure long-term funding and support and ensure that the solution can operate independently of external resources.
- **Be data driven**. Collect, analyse and use data to inform decision making and improve performance.

- **Use open standards, open data, open source, and open innovation**. Adopt interoperable and transparent approaches that facilitate collaboration and sharing of knowledge and resources.
- **Reuse and improve**. Learn from existing solutions and adapt them to the local context and needs.
- **Do no harm**. Assess and mitigate the risks and harms that the innovation may cause to the users, communities and environment.
- **Address privacy and security**. Protect the data and information of the users and respect their rights and preferences.

Ethical innovation is about ensuring that technology is human-centered, inclusive, responsible and impactful. By following these principles, innovators can design solutions that are more likely to achieve social good and avoid unintended consequences.

DATA PRIVACY & SECURITY

Data privacy is the right of individuals to control how their personal data is collected, used, shared and stored by others. Data security is the protection of data from unauthorized access, use, modification or destruction. Data privacy and security are closely related, but not the same. Data privacy focuses on the rights and choices of individuals, while data security focuses on the technical and organizational measures to safeguard data.

IMPLEMENTING BEST PRACTICES FOR DATA PRIVACY AND SECURITY

Here are some of the best practices for data privacy and security for technology for social good:

Assess and classify data. First, assess your business data comprehensively to understand what types of data you have. Then, classify your data according to its sensitivity and the value it adds to your business.

Practice minimal data collection. A rule of thumb when collecting data is to only collect what you need. Avoid collecting unnecessary or excessive data that may increase the risk of exposure or misuse.

Get consent and be transparent. Before collecting or using someone's data, get a clear go-ahead from the user. And this shouldn't be buried in jargon; it should be as clear as day. Let them know why and how you are collecting their data, how you will use it, who you will share it with and how long you will keep it.

Practice robust data security. Use encryption, authentication, access control and other technical measures to protect your data from unauthorized access or loss. Also implement policies, procedures and training to ensure that your staff and partners follow the best practices for data security.

Encourage education and awareness. Privacy can become a way to engage with your customers and show them you respect their data. Educate them about their rights and choices regarding their data, and provide them with easy ways to access, update or delete their data if they wish.

Create achievable policies and SLAs with third parties. If you work with third parties who handle your data, such as cloud providers, vendors or contractors, make sure they adhere to the same standards of data privacy and security as you do. Establish clear policies and service level agreements (SLAs) that define the roles, responsibilities and expectations of each party.

By following the best practices outlined in this article, you can ensure that your technology respects the rights and interests of your users and beneficiaries, while also creating value and impact for your organization and

ADDRESSING ETHICAL DILEMMAS

Identify the stakeholders and their values. Who are the people or groups that are affected by the technology, directly or indirectly? What are their needs, preferences, rights, and responsibilities? How do they value the benefits and risks of the technology?

Analyse the ethical issues and principles. What are the moral values or principles that are relevant to the technology and its use? For example, privacy, autonomy, justice, transparency, accountability, etc. How do they conflict or align with each other and with the stakeholders' values?

Evaluate the alternatives and consequences. What are the possible actions or decisions that can be taken regarding the technology and its use? What are the potential outcomes and impacts of each alternative on the stakeholders and their values? How likely and how severe are they?

Choose the best option and justify it. Based on the analysis and evaluation, what is the most ethical option that balances the interests and values of all stakeholders? How can you explain and defend your choice using ethical reasoning and evidence?

Monitor and revise as needed. How can you monitor the implementation and effects of your choice? How can you identify and address any new or unforeseen ethical issues that may arise? How can you learn from your experience and improve your ethical decision-making in the future?

8.3. ACCESSIBILITY & INCLUSION

THE DIGITAL DIVIDE

The digital divide is the gap that exists between those who have access to digital technology and the internet, and those who do not. It affects millions of people in Australia, especially in remote and regional areas, low-income households, older people, and people who speak a language other than English at home.

The digital divide can limit people's ability to participate in society, access essential services, communicate with others, learn new skills, and find opportunities. It can also increase social isolation, disadvantage, and inequality.

There are ways to bridge the digital divide and promote digital inclusion. Digital inclusion means ensuring that everyone can access, afford, and use digital technology and the internet effectively. It also means helping people develop their digital ability, which is the knowledge, skills, and confidence to use digital technology safely and creatively.

HOW TO MEASURE DIGITAL INCLUSION

One way to measure digital inclusion is to use the Australian Digital Inclusion Index (ADII). The ADII is a tool that uses survey data to measure digital inclusion across three dimensions: access, affordability, and digital ability. The ADII also explores how these dimensions vary across the country and across different social groups.

The latest ADII report shows that digital inclusion at the national level is improving, but there are still significant gaps and challenges. For example, 11 per cent of Australians are "highly excluded" from digital services, meaning they do not have access to affordable internet or don't know how to use it. That equates to about 2.8 million people.

The report also shows that the divide between metropolitan and regional areas has narrowed but remains marked. People in capital cities are more likely to be online than those in regional areas, and unsurprisingly, low-income earners struggle to connect. There are different reasons for the digital divide – many older Australians lack online literacy, while in some areas a lack of infrastructure limits options.

BRIDGING THE DIGITAL DIVIDE

Bridging the digital divide requires a collaborative effort from various stakeholders, including governments, businesses, community organisations, educators, researchers, and users themselves. Some of the strategies that can help bridge the digital divide are:

- Improving the availability and quality of internet infrastructure and services in remote and regional areas
- Providing affordable and flexible internet plans and devices for low-income households
- Offering free or subsidised access to public internet facilities such as libraries, community centres, or Wi-Fi hotspots
- Developing and delivering digital literacy programs that cater to the needs and preferences of different groups of users
- Supporting online safety and security awareness and education
- Encouraging and facilitating online participation and engagement in social, cultural, economic, and civic activities
- Promoting innovation and creativity in using digital technology for personal and professional development

LEGAL & ETHICAL IMPERATIVES

Accessibility and inclusion are not only good practices, but also legal and ethical obligations for organisations that provide products, services or information to the public.

WHAT IS ACCESSIBILITY AND INCLUSION

Accessibility involves designing systems to optimise access for people with disability or other diverse needs. Inclusion is about giving equal access and opportunities to everyone wherever possible, and respecting and valuing diversity.

Accessibility and inclusion benefit not only people with disability, but also other groups such as older people, people from different cultural backgrounds, people with low literacy or digital skills, and people in remote areas.

WHAT ARE THE LEGAL AND ETHICAL FRAMEWORKS FOR ACCESSIBILITY AND INCLUSION?

There are several laws and standards that require organisations to provide accessible and inclusive products, services or information. These include:

The Disability Discrimination Act 1992 (DDA), which makes it unlawful to discriminate against people with disability in various areas of public life, such as employment, education, accommodation, access to premises, goods, services and facilities.

The Web Content Accessibility Guidelines (WCAG), which are internationally recognised standards for making web content accessible to people with disability. The Australian Government has adopted WCAG as the minimum level of accessibility for all government websites.

The United Nations Convention on the Rights of Persons with Disabilities (CRPD), which is an international treaty that promotes and protects the human rights of people with disability. Australia ratified the CRPD in 2008 and has obligations to ensure that people with disability can access information, communication, technology, education, health, employment, justice and other services on an equal basis with others.

Apart from legal compliance, accessibility and inclusion are also ethical imperatives for organisations that want to demonstrate social responsibility, respect for human dignity, and commitment to diversity and innovation .

IMPLEMENTING ACCESSIBILITY AND INCLUSION

To implement accessibility and inclusion effectively, organisations need to adopt a holistic approach that covers all aspects of their operations, such as:

Developing an Accessibility Action Plan that outlines the organisation's vision, goals, strategies, actions, responsibilities, timelines and measures for improving accessibility and inclusion for people with disability as employees, customers and stakeholders.

Making workplace adjustments that anticipate the needs of people with disability and provide reasonable accommodations for individuals, such as ergonomic equipment, assistive technology, flexible working hours and locations.

Communicating and marketing in accessible ways that ensure that all communication channels, such as websites, social media, emails, brochures, videos and podcasts are accessible to people with disability and can be adjusted for individual preferences.

Designing products and services that value people with disability as customers, clients or service users and address their needs when developing and delivering products or services.

Recruiting and retaining people with disability as employees at all levels of the organisation and providing them with career development opportunities.

Engaging suppliers and partners that reflect and enable the organisation's commitment to accessibility and inclusion and expect them to follow best practices.

Innovating practices and processes that continually strive to do better in accessibility and inclusion and seek feedback from people with disability to improve outcomes.

PROMOTING INCLUSIVITY

WHY IS INCLUSIVITY IMPORTANT?

Inclusivity is not only a moral duty, but also a strategic advantage for organizations. By promoting inclusivity, organizations can:

- Enhance their reputation and trust among customers, employees, partners and regulators.
- Increase their innovation and creativity by tapping into diverse perspectives and experiences.
- Reduce their legal and ethical risks by complying with relevant laws and standards.
- Improve their efficiency and effectiveness by avoiding bias, errors and waste.

PROMOTING INCLUSIVITY

Promoting inclusivity requires a holistic approach that involves all stakeholders in the IT governance, policy, ethics and law domains. Here are some best practices that I recommend based on my research and experience:

- Establish a clear vision and strategy for inclusivity that aligns with the organization's mission, values and goals.
- Define and communicate the roles and responsibilities of each stakeholder in ensuring inclusivity throughout the IT lifecycle.
- Conduct regular assessments and audits to measure the level of inclusivity and identify gaps and opportunities for improvement.
- Provide training and education to raise awareness and skills on inclusivity issues and solutions.
- Implement policies and standards that support inclusivity principles and practices.
- Adopt tools and methods that enable inclusive design, development, testing and evaluation of IT solutions.
- Engage with diverse groups of users, customers, experts and communities to solicit feedback and input on IT solutions.
- Monitor and review the impacts and outcomes of IT solutions on different groups of people and society at large.