Hardware

Specifications of Digital Devices and Their Impact on Usability:

The Main Board:

The main board is the body of the computer that connects all external and internal computers together. For example, RAM, CPU and USBs.

- ➔ Essentially, it is a printed circuit board that houses electric components and provides connections via BUS (a path that information and data will flow through) between these components.
  - It has capabilities for expansion.
    - It is frequently termed “the heart of the computer”.

Central Processing Unit (CPU):

The processor is responsible for executing a sequence of stored instructions called a program.

- ➔ It is divided into two sections:
  - Arithmetic and Logic Unit (ALU) = adds, subtracts, multiples and divides numbers, then compares these mathematical values.
  - Control Unit = interprets these numbers, and takes inputs from devices, processes these inputs, then outputs these into an output device.

The steps the CPU takes to function can be simplified into the following:

1. Fetch – gets an instruction from the computer.
2. Decode – gets the appropriate variables needed for the execution of these instructions.
3. Execute – completes the result of these instructions.
4. Memory – memory is written/ read for instructions that require so.
5. Write Back – Writes data and outputs the result.

Random Access Memory (RAM):

RAM is a type of computer memory that comes in different forms; it can be read and altered in any order. Random access memory is the major form of primary memory:

- ➔ Primary = consists of the cache and RAM.
  - This is accessed directly by the CPU, allowing significantly faster access times from the RAM to the CPU, as opposed to from secondary memory to the CPU.
    - This data is volatile. It will not be retained when depowered.

How Random Access Memory Works:

Memory is stored in cells/ memory bits (also known as binary digits).

- ➔ Binary Digits are Bernoulli variables that either take on the form of 1 or 0, denoting notions such as True/ False and Yes/ No.
  - All these bits in the memory are directly accessible whenever, hence the term random access memory.

Random Access Memory can be split into:

- ➔ Static RAM = the memory within the CPU, this is commonly known as the cache.
  - A large cache is expensive, due to its proximity to the CPU and ability to function at three times the speed of other memory types.
- ➔ Dynamic RAM = regular RAM that consists simply of a transistor and capacitator.

From this, a time can be calculated from memory that is transported from the memory banks to the RAM – this phenomenon was coined as latency.

- ➔ This dictates how expensive a cache can be; RAM prices are usually indicative of the latency of the device.

The Hard Drive:

The hard disk drive (HDD) is a computer storage device containing a variety of magnetic disks rotating at high speeds. HDD is the major form of secondary memory:

- ➔ Secondary = stores information that is not frequently accessed by the operating system. Consists of the HDD, SDD and thumbdrives.
  - They are characterized by their superior storage capacity, compromising on their access speed as a result.
    - This data is non-volatile. It will be retained when depowered.

Graphics Card:

The graphics card is a form of processing unit that converts information to colour output on a display. Like most components, it is connected to the motherboard.

- ➔ It has its own RAM.
- ➔ They often include a means of video output such as HDMI and DVI to enable connection to an external display.

Power Supply Unit (PSU):

The power supply unit converts main AC to lower voltages. It regulates DC power for the internal components of a computer.

- ➔ It ensures that is there a consistent supply of voltage and hence, a consistent supply of power to the device.
  - These units can also act as a battery – these are specifically called uninterrupted supply units.

Network Interface Card (NIC):

The network interface card provides a computer with wired and networking capabilities. NICs are also connected to the motherboard.

Mobile Employee Considerations – Usability:

A mobile employee would require the following:

- ➔ Wireless Internet and/ or data services = Wi-Fi and data services are essential to the functioning of an employee in all work environments, on-the-go and in the office.
  - Without this, productivity would significantly decrease as a disconnected employee is constrained by the environment in which he works.
    - In essence, they would be unable to carry out business tasks outside the office etc.
- ➔ Weight = the weight of the device must be such that it can be easily carried around and portable, irrespective of the environment.
  - A lightweight size for laptops for instance, is under 1KG.
- ➔ Battery Life = 8-10 hours would suffice; this is the average hour a full-time employee works.

In relation to the characteristics of the device, they should require:

- ➔ Mid-tier Processing Power = users who are mobile will undergo lengthy periods of time without access to charging ports or power, hence, a CPU should be selected based on its ability to carry out simple tasks and alleviate the device's battery of 'hassle'.
  - A strong CPU consumes a lot of batter life.
- ➔ 'Fair Amount' of RAM = RAM should be selected based on the functioning of the device, bearing in mind that a large amount of RAM will also reduce battery life.
  - The RAM usually for mobile users only has to carry out simple, multitasking functions.
- ➔ Small-sized Screen = A screen size should be selected based on the portability and usability requirements of the mobile employee.
  - A large screen size will add unnecessary visual real-estate, increase the weight of the device and inhibit the mobile nature of this device.

Examples of devices for mobile employees include the Microsoft Surface Pro, the iPad and a Samsung Galaxy S10.

Graphic Designer/ Gamer Considerations – Usability:

A graphics designer/ gamer would require the following:

- ➔ Battery Life = due to the strenuous tasks that these devices will be subjected too, it is a fair assumption that their workstations will be stationary and hence, plugged into power at all times.
  - Battery life is not at the forefront of this demographic's attention.
- ➔ Weight = this device won't be transported regularly and is likely to remain in its location once setup.
  - Weight also is not at the forefront of this demographic's attention.

In relation to the characteristics of the device:

- ➔ Large Screen-size = graphics are essential to both gamers and graphic designers, hence their screen size should be selected depending on how large they believe their screen needs to be to house their visual content.
  - 27-inch monitor screens are an industry standard.
- ➔ Powerful Multi-core Processor = the processer must be able to carry out multiple tasks simultaneously and rapidly provide outputs when inputs are made.

- The current generation of Intel processor, the Intel Xeon, is an octacore processor that gamers frequently adopt due to its reliability.

➔ Powerful Graphics Card = as said previously, graphics exist at the core of this demographic and it is essential that a graphics card is selected that provides a vibrant output of colours and has a variety of output media.
- AMD Fire Pros are a standard that offers multiple video outputs, HDMI and consists of around 2GB of VRAM – a girthy amount albeit.

➔ High Performance Networking = Wireless 802.11AC is the most up-to-date wireless standard, and when combined with Gigabit ethernet ports and thunderbolt capabilities, this demographic is able to easily access and maintain online connections.

Characteristics of Development Trends in Emerging Mobile Devices:

Fingerprint Scanners:

Fingerprint scanners have ushered in a new generation of device protection and unlocking – this unveiling a profound dimension of unlocking mechanism unseen in decades previously.

➔ Fingerprint scanners work by scanning the ridges of the end of your finger, and creating a digital image of this and establishing this as password for future device access.
- Multiple devices nowadays employ this technology, such as Commonwealth Bank's netbanking app.

Businesses should consider integrating this technology in their business as it remedies the need to remember complex passwords.

➔ Equally, the implementation of fingerprint security increase the likelihood that passwords are forgotten as they become superseded, preventing future access to devices that may not have fingerprint technology.

Wearable Technology:

Wearable technology is a concept that is evidently self-explanatory; it is technology that you wear on you, functioning as an 'extension of the body'.

➔ Devices such as smart watches, smart glasses all contain means of easy access to notifications, communication and fitness tracking.

Businesses can employ wearable technology to monitor the productivity and health of their workplace, such as their total steps per day etc.

➔ This would allow health to gain primacy within the business and foster an environment that reinforces the life facet of the work-life balance.

Near Field Communications (NFC):

NFC is a new wireless technology that has recently gained ascendancy in their popularity and their incorporation in device design.

➔ NFC has paved the way for features such as Apple Pay to become successful; in this case, it allows users to pay via smartphone or watch.

- This sort of technology is more secure than PayPass technology as it requires a pin/ passcode before the authorization of a transaction. If the device is stolen, it cannot simply be tapped for payments like PayPass devices can.

Apple Beacon has recently gained media traction in its clever use of NFC technology.

➔ It uses NFC to transmit sales, catalogue and business information to customers within the vicinity of the beacon and who have NFC enabled on their devices.
- This allows less customer-retailer interaction, whilst this may seek inauthentic, it may be preferable depending on the circumstances of the customer.
- It also provides an additional realm of advertisement to be reached; users can be enticed into purchasing products without human persuasion.

Virtual Reality:

Virtual reality is a multifaceted medium of graphic entertainment that incorporates both elements of the real and digital world.

➔ Usually is allows users to record real-time environmental aspects and combines them with virtual features typically accessed through devices like the Oculus Rift of device camera.
- Another version of virtual reality which does not consist of the same number of visual elements is augmented reality.
  - Augmented reality = the real-time environment is intensified by the presence of a few visual elements.
    - Pokémon Go is a prime example of augmented reality.

It can be utilized as a military technology. Immersive 360° video can allow for virtual training simulations as well as open up possibilities of '4D', interactive cinema.

Usability of Digital Devices for Specified Client Requirements:

Power and Performance:

To perform basic functions, 2GB of RAM would be enough for mobile phones to allow them to multitask, while laptops need a minimum of 4GB to function.

➔ Complex tasks are usually reserved for desktop use on business premises.
➔ Mobile devices must have a decent CPU to ensure the upholding of social standards in relation to day-to-day tasks, such as: emails, word processing and light editing.

Weight and Portability:

Ideally, a light device is preferable as an employee is than easily able to transport it in a mobile environment.

A heavy device would inhibit its transport and location, however, offers the benefit of:

➔ Constant charging,
➔ Less load to carry when moving,
➔ No need for cellular data when outside Wi-Fi range.

Whilst some devices such as iPad Pros are classified as mobile devices, their use as a mobile device is limited due to its screen size etc.

Battery Life:

Mobile devices are typically designed to have a battery life of 8 hours of extended usage – the typical employee working day,

If they are bound within a certain area, then the battery life would not be at the forefront of the users attention because more often than not, there would be a charger in the close vicinity.

Internet Accessibility and Speed:

Majority of mobile devices are equipped with Wi-Fi capabilities.

➔ This typically comes in the form of 802.11ac for fast download speeds.

Furthermore, these devices are also equipped with mobile data capabilities, allowing internet access without Wi-Fi.

➔ This is advantageous to those who work rurally, off-site or constantly travelling as they would not have a consistent Wi-Fi connection throughout the course of their day.
- Cellular data provides an additional facet of mobile downloading and uploading previously unseen in years previous.

User Interaction Medium:

Laptop users cannot work unless there is suitable physical support.

Mobile devices can have touchscreen capabilities, and sometimes a stylus.

Cost:

Newer technology quickly supersedes older models, which depreciate in value.

Best Practices for Designing an Interface:

1. Keep the interface simple.
   - Avoid unnecessary elements and be clear in language.
2. Use common UI elements with consistency.
   - Patterns in design should create familiarity amongst viewers.
     - It should also facilitate efficiency – users should be able to transfer their skills across the site.
3. Strategic use of Colour and Texture.
   - Colour and texture can be used to direct or redirect the attention of users.
4. Typography, Hierarchy and clarity.
   - Typeface, size, font, and arrangement can combine to increases scanability, legibility and readability.
5. Purposeful page layout.
   - Consider spatial relations between items.
     - Items carefully placed can draw attention to the more important pieces of information and simultaneously redirect their attention away from superfluous content.

W3C Standards in Relation to Design:

Usability:

The designing of an ICT product to be effective, efficient and satisfying.

Examples of this include:

- ➔ Search bars = Allows for quick access to desired content.
- ➔ Simple and Consistent Design = provides familiarity and predictability to the design, enhancing navigation.
- ➔ Thumbails = provides snapshots of content to those with poor bandwidth.

Inclusivity:

Inclusivity refers to the involvement of everyone to the greatest extent possible without adaptation; enhancing the diversity of the digital solution.

Examples of this include:

- ➔ Language translator = allows for the target audience to now include those of differing language.
- ➔ Currency converter = allows those living within different economic systems to still access and view prices like everyone else – sameness.
- ➔ Font enlarger = increases size of font to prevent squinting and to assist those with visual impairment.

Assistive and Adaptive Technologies:

Assistive Technologies:

Assistive technologies are software and hardware that allow people with disabilities to interact with the web on a equal plane of those without disabilities.

Examples of these include:

- ➔ Screen readers = enable blind people to hear content that they cannot read by reciting it loudly through the devices speakers.
  - These cannot read images however, hence the need for alt-text.
- ➔ Magnification software = increase the size of a portion of the user's screen in order to increase visibility.
- ➔ Alternative (braille) keyboard = can assist those with visual impairment by allowing them to access desired content in their own language.
- ➔ Voice recognition software = allows the human voice to active certain commands on a device.

Adaptive Strategies:

Adaptive technologies differ from assistive technologies in that these strategies are provided by the device, and they are not additionally downloaded or purchased.

Examples of these include:

- ➔ Increasing text size = a windows standard feature that assists the visually impaired.
- ➔ Reducing mouse speed = assists those with poor fine motor skills.
- ➔ Captions = assists those with auditory problems.

Accessibility:

Addresses discriminatory aspects of design and remedies them, to allow equal user experience and to allow them to perceive, operate and understand content without needing assistance.

Examples of this include:

- ➔ Captions on multimedia = those with auditory impairments or those who are simply deaf, are given textual alternatives to videos and audio to allow them to understand content.
- ➔ Keyboard navigation = special markings on the keyboard is used to allow blind users to navigate using keyboard inputs.
- ➔ Audio narrator = Helps the blind by aurally reciting text to them.
- ➔ Saved login credentials = assists those with memory loss by keeping login data for them, rather than them being forced to remember it.
- ➔ Font enlarger = increases the font size to assist those with optical impairments.
- ➔ Large buttons = thumb-friendly design allows for the demographic with poor fine motor skills to navigate through the content with success.

Accessibility Guidelines

➔ Perceivable.
- Text alternatives are provided for non-text content.
- Captions for multimedia.
  - Alt-text.
- Creates content that can be presented in different ways.
- Makes it simple for users to both see and hear content to assist those who are impaired.

➔ Operable.
- Functionality should also be present with the keyboard; users should be able to navigate using keyboard navigation controls.
- Users should be given enough time and visual real estate to view and digest content.
- Signposting and other means of visual prompts should be present to help users navigate and find content.

➔ Understandable.
- Text should be made readable and understandable.
  - Simplistic lexicon and large font size.
- Content should assist users in avoiding and correcting mistakes.
- Content should be predictable and a sense of familiarity with content should pervade.

➔ Robust.
- Maximize compatibility with browsers and user tools.

Design Concepts

Relationship(s) Between the Elements and Principles of Design:

Elements of Design:

- ➔ Line = linear marks within a design, joining points together.
  - They can be horizontal, vertical, diagonal, curved, thick, thin etc.
- ➔ Shape = 2D objects with no form or thickness.
  - Can be organic or geometric shapes.
- ➔ Space = refers to variations in the proportions of objects, lines or shapes.
- ➔ Texture = concerns the surface quality of an image, either tactile or visual.
  - Put simply, it is the degree of roughness or smoothness in objects.
- ➔ Colour = specific hues used and their properties.
  - Tints come about from adding white to a colour.
  - Shades come about from adding black to a colour.
  - Tones come about from adding gray.
- ➔ 3D-Form = 3-D dimensional objects having volume and thickness.
  - It can be implied through lighting and shading techniques.
- ➔ Tone = the degree of light and dark in a design; denoting extreme changes between values.

Principles of Design:

- ➔ Balance = refers to the visual weight of the elements of the composition. This can be achieved in four ways:
  - Symmetry = mirrored designs and design elements.
  - Asymmetry = the contrast of design elements.
  - Radial symmetry = equal spacing around a centre point in a design.
  - Negative space = negative space can be juxtaposed with positive space when they are both proportional to each other, to create balance.
- ➔ Movement = the product of elements of design used that move the viewers eye around and within the image. This is created by:
  - Repetition of similar sized shapes.
  - The use of lines to guide the viewers eye.
- ➔ Emphasis = the creation of an area which is visually dominant and commands the viewers attention. This can be achieved by:
  - Contrast of elements of design.
  - Contrast of size proportion of elements of design.
- ➔ Dominance = the alteration of the size or colour of an element present in a design to bestow a larger visual weight onto that element in comparison to other elements in the design – this is usually the focal point. This is made through:
  - Large objects in a design.
- ➔ Unity = the equilibrium between the areas of interest in a composition and places of little visual importance. This comes about from:
  - A consistent colour scheme.
  - Repetition of similar sized shapes.
- ➔ Pattern = the uniform repetition of any of the elements of design.

The Combination of Elements and Principles of Design:

Principles of design do not exist in a vacuum; they are products of the presence of design elements within a composition.

➔ Without design elements, principles would not exist – design elements construct design principles.

Features of a User Interface:

Logical and Hierarchical Organization of Content:

When creating a digital solution such as a webpage, there are three areas of design that can be considered for the placement of content:

➔ Upper quartile of design.
- This section contains content that the user will be immediately and initially exposed to.
  - Designers can tactically place elements here for immediate recognition of elements.
    - For example, business names, address, phone number, information about sales etc.
- Anything for the sake of easy access of information, efficient marketing and encourages a positive user experience (UX) should be placed here.

➔ Middle quartile of design.
- This section should contain content that supports the purpose of the business website.
  - For example, customer testimonials, email subscriptions, contact forms, social media widgets etc.

➔ Lower quartile of design.
- Should provide assistive information that may not directly affect the purpose of the business website.
  - This comes in the form of copyright and privacy acts, terms of use and other legal and additional information.

Graphical User Interface (GUI) Suitable for Target Audience:

Input Controls:

Input controls are essential features of any form; they allow users to perform a variety of functions such as type in text, select items from a list, upload files etc.

Examples of these include:

➔ Checkboxes = allow users to select options from a set.
➔ Dropdown lists = allows user to select an item from a series of choices.
- More compact than radio buttons, saving visual real estate.

➔ Buttons = indicates an action up touch, usually denoted by text, an icon or both.
➔ Text fields = allows users to enter single lines or multiple lines of text.

Navigational Components:

Navigational components are browsing tools that allow users to choose where within a website's interface they want to go.

Examples of this include:

➔ Search field = a box that allows users to enter a keyword or phrase, prompting the system to index said text and to respond with the most relevant results.
➔ Breadcrumbs = provides visual representation and a clickable trail of the users current and previous location on a webpage.

- ➔ Pagination = divides content into multiple webpages and allows users to click numbers emblematic of the page numbers of content, to browse the website.
- ➔ Icons = a simplified image serving as an intuitive symbol to aid user navigation.
- ➔ Image carousel = provides a compact slideshow of images, typically showcasing products and items that can be selected.

Informational Components:

Informational components are aspects of a webpage that are educative and aim to assist the user in comprehending information present.

Examples of this include:

- ➔ Notifications = an update message that announces new information to users.
- ➔ Progress bars = a visual representation of a series of steps undertaken on a website, indicating where users are currently.
- ➔ Tool tips = provides hints or assistance when hovered over.

Containers:

Refers to the area/ 'box' that information is contained within.

Examples of this include:

- ➔ Accordion = a vertically stacked list of items that utilizes show/ hide functionality. It can be expanded to show content

Application Skills

Online Software Tools:

Online software tools are programs that can be accessed and used when directly connected to the internet.

Advantages of Online Software Tools:

- ➔ Users are no longer confined to a working environment.
  - Work software can be accessed from anywhere with an internet connection, as opposed to be being limited to business premises.
- ➔ There is no need to download or install software.
  - Online software availability alleviates the need for downloading software to the user's device.
- ➔ Periodic updates are usually available, and no software maintenance is required.
  - Online tools are frequently updated, and no additional downloads are needed to access this.
  - Issues with the software are no longer the user's responsibility.

Disadvantages of Online Software Tools:

- ➔ Poor connectivity will inhibit functioning of online software tools.
  - A weak internet connection will slow down these tools and inhibit productivity.
- ➔ Product may be insecure and lead to privacy issues.
  - Information may need to be shared with the providers of these tools, potentially jeopardizing the user's privacy.

Video Application Features:

Multilayer Track Editing:

Whilst usually a single video track is sufficient for editing, multiple layers can be used to enhance creativity and split a project into workable proportions.

- ➔ Multiple layers also allow for efficient editing in that layers can be grouped by purpose or content.
  - Also allows for video effects to come about such as opacity and blend mode features, and filters too.

Transitions:

Transitions are the joining of two shots or clips via video effects such as fades, dissolves, instants etc.

Effects:

Visual effects provide aesthetic appeal and interesting transitions from scene-to-scene.

- ➔ This is primarily achieved upon image manipulation and filter effects.

Publishing Features:

Typography:

The art of arranging content language in a legible and readable fashion while also being appealing when displayed. More specifically, it refers to the:

- ➔ Typeface = the particular design type of text – a collection of letters forming a pattern through patterns.
- ➔ Size = the magnitude of the font and the amount of visual real estate it occupies.
- ➔ Alignment = refers to the position that the text occupies.
- ➔ Spacing = related to the space in-between and surrounding the letters.

Print/ Display Options:

RGB:

RGB stands for Red, Green and Blue and was the first print/ display option presented for the web.

- ➔ It has the potential to output millions of colour, all mixed from red, blue and green.

CYMK:

CYMK stands for Cyan, Yellow, Magenta and Key (black).

- ➔ It is a newer display option that many monitors now support and use.
  - It has a limited range of colours however.

Digital Publications:

Electronic Publication (EPUB):

Electronic publications are pretty self-explanatory – the definition is in its name.

They are particularly advantageous over traditional printed publications in that they have:

- ➔ An easy layout to follow.
- ➔ Can be adaptable to different screensizes and zoom features are also standard.

Their shortcomings come in that:

- ➔ They can sometimes be presented in a format that is unrecognizable or incompatible with the user's device.
- ➔ They can be incorrectly displayed on some displays.
- ➔ Requires an internet connection to download and access.

Impacts of Technology (1)

The Concept of Intellectual Property (IP):

Intellectual properties are defined as intangible properties that are the result of creativity, such inventions, literary and artistic works, images and the like.

- ➔ It is essential that these are protected to foster growth in areas such as research, innovation and employment.
  - This encourages new technologies to be created and newer means of artistic expression.
    - This simultaneously promotes economic growth.

Intellectual Properties allow owners the right to:

- ➔ Exclusively exploit the product for commercial gain.
- ➔ Prevent others from unauthorized copying and distribution.
- ➔ Gives ground for legal compensation for unauthorized use.

Intention and Purpose of IP in Australia in relation to Copyright and/ or Design of Digital Products:

- ➔ Patent = protects how an invention works or functions.
  - When granted, a patent will give you exclusive commercial rights to your invention, can last up to different periods of time – this can result in ideas for innovation 'running out'. **Patents Act 1990.**
- ➔ Trademarks = a legal document which grants the owner exclusive commercial rights to a keyword or phrase of keywords as a way of identifying a unique product or service.
  - Logos, words, letters, scent, picture, advertising etc. are protected by this. **Trademark Act 1995.**
- ➔ Registered Design = the recognizable visual appearance of a product is protected but not the way it works.
  - For example, Adidas shoes. **Design Act 2003.**
- ➔ Plant Breeders Rights (other) = to protect the commercial rights of new plant varieties because of the time spent by companies on the manufacturing of specific genes.
  - For example, ST26 Grass.
- ➔ Trade Secrets (other) = protected secrets.
  - For example, KFC secret herbs and spices and the formula for Coca-Cola.
- ➔ Copyright = this will be defined later… **Copyright Act 1968**

The Concept of Online Defamation in Australia:

The action of damaging the good reputation of someone; slander or libel. This comes in the form of:

- ➔ Say you are dishonest or disloyal,
- ➔ Ridicule you,
- ➔ Accuse you of committing a crime, or
- ➔ Say you have a diseases or sickness.

More specifically, online defamation is the process of publishing untruths about someone on the internet with the purpose of intentionally causing harm and damage a person's reputations.

Examples of online defamation:

- ➔ Someone posts publicly a sexually explicit photo of you without your permission.
- ➔ Someone states online that you are a criminal despite not having a criminal record.
- ➔ Someone falsely accuses you of harassing them by posting an online social media status.

To defend against defamation, you can:

- ➔ Claim the information is substantially true.
- ➔ The information is published with the consent of the person being defamed, or
- ➔ The information wasn't very important; it is unlikely that the person's reputation will actually be damaged.

Legal Action Available in Australia to Counteract Online Defamation:

If you are defamed:

1. Record all evidence of online defamation.
   - Recording evidence online provides legal security in the event legal action is required to take place.
     - Evidence can be used as grounds for legal action and demands for compensation.
2. Block user.
   - Immediately block the user, however this may remove the ability to record evidence for further online defamation.
3. Report content.
   - Online defamation victims should report the content to website administrators who should remove the content
4. Contact legal advice.
   - Victims can seek legal advice because under the **Defamation Act 2005**, victims have the right to sue, and in some cases, criminally charge perpetrators.

If you are accused of defamation, you should:

- ➔ Remove the material immediately,
- ➔ Offer to publish a reasonable correction,
- ➔ Offer to pay expenses reasonably incurred by the complainant to the time of the offer,
- ➔ An apology can be useful.

The Concept of Freedom of Information (FOI) in Australia:

The Freedom of Information Act 1982 is administered by the Office of the Information Commissioner (OIAC) and allows an individual the right to access personal documents or documents in the public interest held by government ministers and agencies etc.

- ➔ It ensures government transparency.
- ➔ Encourages active individual participation with government.

Key Provisions of FOI in Australia in Relation to Digital Products:

You can request a variety of information under Freedom of Information:

- ➔ Medical records,
- ➔ Non-confidential government documents,
- ➔ Personal documents relating to the individual e.g. credit history.

To access information/ appeal against a decision:

1. An appeal must be made in writing.
2. An electronic address must be provided for where the agencies can send their decision.
3. The request will need to state it is under the Freedom of Information Act.
4. To make a valid request, you will need to complete a form.
5. A decision will be acknowledged within 14 days and a decision will be reached within 30 days of submission of the application.

In relation to the hierarchy of the FOI request, it goes through an:

Administration officer → Manager of department → Information commissioner → Ombudsmen.

Key Provisions of the Freedom of Information Act in Relation to Digital Products:

1. It allows access by the general public to data held by national governments, under the FOI act, you have a legal right (subject to some exceptions) to see documents held and get copies of those documents.
2. Information accessed is accessible very fast and classified within the storage environment.
3. It is vital that the physical storage of data is free from the elements.
4. Digital data must have virtual security to protect it from cyber-hacking.
5. Information access can only be granted to the 'right' people who will be able to get and make use of the data in a timely manner.

Exceptions of Freedom of Information Act:

- ➔ National security risk = any sensitive information that is regarded as a national security risk, such as documents helped by the Australian Defence Force cannot be released.
- ➔ Documents disclosing trade secrets = any sensitive information that contains details about trade and foreign economy affairs are excluded.
- ➔ Private documents = Freedom of Information applies only to government documents, documents held by private entities cannot be accessed.
- ➔ Documents whose disclosure would be in contempt of parliament or in contempt of court.
- ➔ Contains information about other individual that isn't relevant to yourself.

➔ Documents where disclosure could reasonably be expected to prejudice an ongoing investigation.

Advantages, Disadvantages and Implications of Virtual and Physical Collaboration:

Virtual Collaboration:

Virtual collaboration is the usage of online technology for communication between two or more people in different geographical locations.

Advantages:

➔ Reduced cost = businesses no longer need to rent out office space nor organize meetings to collaborate with colleagues.
  - Video calls and online collaboration platforms like Trello and Google Docs can be employed for this purpose.

➔ Delayed communications = employees can maintain a conversation without vis-à-vis communication and can reply when they please.

Disadvantages:

➔ Security vulnerabilities = it becomes easier for hackers to access and record online conversations, data and projects.
➔ Ownership issues = files created and used collaboratively brings up the issue of ownership – who should be credited as the owner of the document etc.?
➔ Additional training = employees may need to be taught how to use new software and technology.

Examples of Virtual and Physical Collaboration:

➔ Board based systems = project management software = Trello.
➔ Face-to-Face communication = Skype.
➔ Text-based live communication = Snapchat.
➔ Messages = Outlook.
➔ Shared documents = Office 365
➔ Storage = cloud = GoogleDrive.

Impact of Convergence Trends in Contemporary Digital Technologies:

Digital convergence refers to the combining of two or more technologies into one device.

Examples of converged devices include:

➔ A smart phone with communications, camera, portable gaming device, audio receivers,
➔ A smart TV, web browser, media streamer and television functionality,
➔ A smart watch, fitness tracker, notification reader, camera and watch functions.

Advantages:

- ➔ Lower volume of household devices = for example, smartphones reduce the need to have separate camera and phones.
- ➔ Increased rate of obsolescence = rate of digital convergence has posed older devices with less functions as obsolete, increasing volumes of environmental waste.
- ➔ Cost savings = households do not have to purchase multiple devices and can purchase one device for all, usually at a lower cost.
- ➔ Increased dependency on a single device = the smartphones ability to perform multiple functions has led to increased dependency on the single device for our digital lives.
- ➔ Greater connectivity (Internet of Things) = convergence of devices has seen smarter homes and workplaces with automated and smart functions, improving standards of living.

Networks

Types and characteristics of communication protocols:

Transmission control protocol/ internet protocol (TCP/ IP)

TCP is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data.

- ➔ TCP works with the Internet Protocol (IP) which defines how computers send packets of data to each other.
  - Together, TCP and IP are the basic rules defining the Internet.

e.g. if you had to separate networks connected together by a router, the connection between the two routers would use TCP/ IP to communicate with one another.

In essence, the IP is the address of a house and TCP is the mailman that delivers the letters to these houses.

- ➔ Private IP = the IP address used by a router to identify your device on a private network, often in the form of 10.1.1.x or 192.168.1.x
- ➔ Public IP = the IP address used to identify your network on the Internet.
  - It can be found by searching ‘what’s my IP’ on Google.

Hypertext transfer protocol (HTTP)

HTTP is the underlying protocol used by the World Wide Web and this protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

e.g. if you access a website “X”, you would have to:

1. enter HTTP which tells the web browser that this address is a web server.

2. the device sends data packets communicated via HTTP.

3. the server responds back with data packets showing the website.

Hypertext transfer protocol over secure socket layer (HTTPS)

Hypertext Transfer Protocol Secure (HTTPS) simply means there is a secure channel where the regular HTTP process has taken place.

- ➔ The data packets are encrypted through public key infrastructure,
- ➔ This involves a private key known by you and the web server and a public key obtained off the web.
  - This ensures that data packets can only be read by the sender and its intended recipient.

e.g. websites such as Commbank, use HTTPS – HTTPS represents a secure channel for data packets to be sent directly from your device to the Commonwealth Bank web servers. Information is encrypted and cannot be read by intruders such as hackers and can only be read by the bank and you.

Wireless application protocol (WAP)

WAP is a communications protocol that is used for wireless data access through most mobile wireless networks.

- ➔ WAP enhances wireless specification interoperability
  - This facilitates instant connectivity between interactive wireless devices (such as mobile phones) and the Internet.

Types and characteristics of communication standards, including:

802.11x (wireless)

Wireless 802.11.x is the Wireless standard to how two devices use radio waves to communicate with one another.

- ➔ 802.11.n = Wireless standard with a maximum speed of around 900MB/s and capable of dual band wireless both 2.4 and 5 GHz frequencies.
- ➔ 802.11ac (latest) = Wireless standard with a maximum speed of around 1300MB/s and support for dual band wireless of both 2.4 and 5 GHz frequencies.

Dual-band wireless

Dual band wireless is aimed at reducing interference because many devices such as microwaves use 2.4 GHz bands, which makes the frequency congested and slower.

- ➔ 5GHz is used by fewer devices and has a greater speed due to a shorter wavelength, however, the range capabilities does decrease as a result.

802.3 (ethernet)

Ethernet 802.3 states that no device has control of data flow in a network and that devices send data packets when network communications become readily available.

- ➔ If a data collision occurs, then data packets are reset until it is successfully transferred.

Types of network security measures:

Firewalls

Firewalls are hardware, software or a router that monitors the incoming and outgoing data packets of a network and rejects any unauthorized data packets.

- ➔ Essentially, a gatekeeper for what packets of data enter or exit a network.
  - It can even ban certain protocols e.g. File Transfer Protocol (FTP).

Passwords

Domain names are used to denote a subset of the Internet, where there is a designated admin who has authoritative control over that domain.

Passwords are a combination of characters, often associated with a username, used to unlock certain computer resources – they are access codes to enter these domains.

Physical security

- ➔ Locked servers = servers should be stored in cages and locked to prevent unauthorized access.
- ➔ Video surveillance
- ➔ Restricted access to server rooms – this can be done through keycards or biometric security
- ➔ Locking doors after use

Topologies:

Wired Star Topology

The wired star topology is one of the most common network setups.

- ➔ In this configuration, every node connects to a central network device, like a hub, switch, or computer.
  - The central networking device acts as a server and the peripheral devices as clients.
- ➔ Depending on the type of network card used in each device, a coaxial cable or a RJ-45 network cable is used to connect computer together.

Advantages:

- Centralized management of the network, through the use of the central computer, hub or switch.
- Easy to add another computer to the network.
- If one computer on the network fails, the rest of the network continues to function normally.

Disadvantages:

- Can have a higher cost to implement, especially when using a switch or router as the CND.
- The central network device determines the performance and number of nodes the network can handle.
- If the central computer, hub or switch fails, the entire network goes down and all computers are disconnected from the network.

Ring Topology

A ring topology is a network configuration in which device connections create a circular data path.

- ➔ Packet travel is only in one direction, called a unidirectional ring. Some are bidirectional and allow data to move in both directions.
- ➔ A coaxial cable or RJ-45 network cable is used to connect computers together.

Advantages:

- All data flows in one direction, reducing the chance of packet collisions.
- A network server is not needed to control network connectivity between each workstation.
- Data can transfer between workstations at high speeds.
- Additional workstations can be added without impacting performance of the network.

Disadvantages:

- All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.
- The entire network will be impacted if one workstation shuts down.
- The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches.

Bus Topology

A bus topology is a network setup in which each computer and network device are connected to a single cable or backbone.

- ➔ Usually connected via coaxial cable or a RJ-45 network cable.

Advantages:

- It works well when you have a small network.
- It is the easiest network topology for connecting computers or peripherals in a linear fashion.
- It requires less cable length than a star topology.

Advantages:

- It can be difficult to identify the problems if the whole network goes down.
- It can be hard to troubleshoot individual device issues.
- Bus topology is not great for large networks.
- Terminators are required for both ends of the main cable.
- Additional devices slow the network down.
- If a main cable is damaged, the network fails or splits in two.

Network types:

Local Area Network (LAN):

A LAN connects network devices over a relatively short distance.

- ➔ In TCP/ IP networking, a LAN is often but not always implemented as a single IP subnet.

IN addition to operating in a limited space, LANS are also typically owned, controlled, and managed by a single person or organization.

- ➔ They typically use connective technologies such as Ethernet.

Wireless Local Area Network (WLAN):

A WLAN is a LAN that is connected via wireless as opposed to wired connections.

Wide Area Network (WAN):

A WAN spans a large physical distance.

- ➔ They are a geographically dispersed collection of LANs.
  - A router connects LANs to a WAN.
- ➔ The internet is the largest WAN.
- ➔ Most WANs are not owned by any one organization but rather exist under collective or distributed ownership.

Metropolitan Area Network (MAN):

A MAN is a network spanning a larger physical area than a LAN but smaller than a WAN, such as a city.

- ➔ A MAN is typically owned by a single entity such as a government body.

Key considerations for home networking:

- ➔ All devices connecting to a wireless router must possess a working network adapter.
  - Connecting to wireless router to a broadband modem enables sharing of high-speed Internet connection.
- ➔ Many wireless network routers also allow up to four wired devices to be connected via Ethernet cable.
  - This makes sense when a computer, printer or other device lacks Wi-Fi capability or cannot receive an adequate wireless radio signal from the router.
- ➔ Most Wireless Access Points (WAP) will have no issue supporting a number of wireless devices, however,, the more devices that attempt to use the WAP to access the network, the slower the network becomes.

Media – wireless:

- ➔ **Bluetooth** = short range radio wave up to 3MB/s
- ➔ **UWB (ultra-wideband)** = short range radio wave (up to 10m) – high speed 110MB/s – good for large transmissions e.g. videos.
- ➔ **IrDA** = Infrared light waves – needs line of sight and speed of 115KB/s
- ➔ **WiMAX** = Worldwide Interoperability Microwave Access – 802.16 standard – long distance – ranges from 15MB/s to 40MB/s

Advantages:

- Mobility = allows its users to remain mobile and hot-spots are becoming a more frequent occurrence.
- Fast setup = as simple as owning a device with a wireless adapter and pressing “connect to network”
- Cost = more cost effective, as opposed to purchasing and installing cables.
- Expandable = you can theoretically add as many devices to the network as you want.

Disadvantages:

- Risk of security breaches = ensure data is protected and backed up.
- Interference = ensure electrical devices near by are switched off and the path of transmission isn’t blocked.
- Speed = Ethernet connections are always faster than wireless connections.

Media – cabled:

Twisted Pair:

A twisted pair consists of multiple twisted wires, paired together and twisted to reduce noise.

- ➔ Cat 5 = 5x twisted pairs.
- ➔ Cat 6 = 6x twisted pairs.

Shielded Twisted Pair (STP) cable:

Unshielded Twisted Pairs (UTP), whilst they are cost-effective, they are susceptible to radio and electrical frequency interference.

- ➔ Hence, STP cables are used to allow network connections in extremely sensitive environments.
  - This includes environments that are subject to torrential weather etc.

Coaxial Cable:

A coaxial cable is a single wire that is surrounded by an insulator and woven with braided copper or aluminium.

- ➔ The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.
- ➔ It is highly resistant to signal interference, however, it is difficult to install.
- ➔ It can support greater cable lengths between network devices than Twisted Pair cables.

Fibre-Optic Cable:

Fibre Optic cables consist of hundreds of thin strands of glass that uses light to transmit or carry data.

- ➔ It transmits light rather than electronic signals, thus eliminating the problem of electrical interference.
  - This immunity makes it ideal for environments that contain large amounts of electrical interference.
  - Also makes it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

- ➔ Has the capability to transmit signals over much longer distances than Coaxial and Twisted Pairs.
  - It also carries information at vastly greater speeds.
- ➔ The cost of Fibre-Optics is comparable to copper cabling.
  - It is difficult to install and modify however.

Impacts of Technology (2)

Data and information security related to personal or sensitive information:

Personal Information:

Personal information is any information that can be used to identify you. Personal information could be characterized as belonging to you.

- ➔ Examples of this include:
  - Address
  - Date or Birth
  - Name
  - Email Address

Sensitive Information:

Sensitive information is information that is protected and should not be disclosed unless under specific circumstances.

- ➔ The Privacy Act is the regulation that defines sensitive information, and it concerns:
  - Racial or ethnic origin
  - Political opinions
  - Membership of a political association
  - Religious beliefs or affiliations
  - Philosophical beliefs
  - Membership of a professional or trade association
  - Membership of a trade union
  - Sexual preferences or practices
  - Criminal records

Security of Personal and Sensitive Information:

Businesses and Government organizations have a legal obligation to protect the personal and sensitive information collected about their customers and citizens.

- ➔ Unauthorized access of personal and sensitive information could lead to identity theft and fraud, amongst other issues.

Challenges of Digital Security:

Before the domination of the Internet, data, both physical and sensitive, was stored physically making security easier to manage.

- ➔ Video surveillance could detect who accessed data.
- ➔ A missing document would be easily noted.

The digitalization of data is now being more prominent and is double-edged by nature. Whilst it allows for improved access by organizations to their data, it poses significant internal and external threats not observed previously.

➔ Data can be accessed discretely by anyone without detection.
➔ Internet connections also bring threats of global hackers located around the world.

Means to Secure Digitalized Personal and Sensitive Information:

Ways in which data can be secured include:

➔ Physical security:
- Video surveillance of server rooms to monitor the accessing of data.
- Keycards and biometric security to restrict access to data.

➔ Electronic Audit Trails = a secure, computer generated, time-stamped electronic record that allows reconstruction of the course of events relating to the creation, modification and deletion of an electronic record.

➔ File Permissions = access to personal and sensitive information can be restricted to authorized users.
- Can be password protected.
  - Passwords are a combination of characters, often associated with a username, used to unlock certain computer resources – they are access codes to enter certain domains.

➔ Firewalls = hardware, software or router based and monitor incoming and outgoing data packets and blocks unauthorized data packets.
- Essentially, a gatekeeper for what packets of data enter or exit network.
  - It can even ban certain protocols e.g. File Transfer Protocol (FTP)

➔ Anti-Virus Software = detects and removes malware on systems that could be used to discretely access personal and sensitive information.

EXTENSION Collectively, threats can be categorized as:

➔ Social Engineering Attacks = cyber-criminals use sophisticated tools such as AI to extract information from corporations and their employee's social media profile.
- This threat is becoming ever-present with the growing usage of the internet.

➔ Supply Chains Attacks = cyber-criminals are now seeking to exploit vulnerabilities in business conduct – rather than target the business itself, they target its vendors, where risks may not be fully understood.

➔ IoT and Infrastructure Attacks = ransomware is likely to be higher as criminals hold companies, cities and even countries hostage as they take over and comprise the legacy systems and IoT devices.
- Attribution will be very difficult due to the multifaceted nature of attacks of this nature.
  - It is very difficult to pin the blame on individuals due to the convoluted nature of these systems – criminals can easily remain unpunished.

➔ Identity and Mobile Authentication = aspects of mobile authentication such as facial recognition and biometrics have not yet reached their apex and are yet to be trusted.

➔ Polymorphic Attacks = day-zero threats – where cyber-criminals exploit unpatched new vulnerabilities at a rapid rate to prevent effective management and remediation of the system.
- This is the most common type of attack and this is expected to continue at an unprecedented rate due to the high demand for software in the marketplace.

Purpose of a code of conduct:

A code of conduct is a set of rules outlining the social norms, religious rules and responsibilities of, and or proper practices for an individual.

- ➔ A company code of conduct is written for employees of a company, which protects the business and informs the employees of the company's expectations. It also serves as justification for disciplinary action where necessary.
    - Regardless of who imposes the code of conduct, there are typically repercussions for those who breach them.

A code of conduct should encourage the discussion of ethnics and improve how dilemmas, prejudices and 'gray areas' that are encountered in everyday work.

- ➔ A code is meant to complement relevant standards, policies and rules, not to substitute for them.

It also serves to clarify the organization's mission, values and principles and links them with standards of professional conduct.

Elements of a code of conduct:

Work hours:

Work hours accept a degree of flexibility within ICT systems. ICT can enable workers to work offsite with remote access to work files and programs, allowing for dynamic access to the business premises.

Employee email use:

Emails sent using an email address licensed by an official company acts under the jurisdiction of the official company policies.

- ➔ Employees should be cautious when sending emails as whatever is sent is legally binding and can be used in the court of the law to enforce contracts or conditions.
    - Whether this acts in the sender's advantage or not is up to them.

Employees should refrain themselves from sending emails with offensive, defamatory, or inappropriate (not limited to this) messages.

Use of the business email address for personal reasons is typically allowed, however, only in moderation and so long as it doesn't have a significant impact on the employee's productivity or of detriment to the company.

Employers have the right to monitor all communications on business email addresses.

Employee internet use:

A company's internet resources can only be used by employees purely for company related purposes.

- ➔ Social media, pornography, gambling or online games violate this code.

Employees are prohibited from using the internet with malicious or illegal motives.

Employers have the right to monitor all traffic on business internet resources.

Employee privacy:

Employees are afforded a degree of privacy in that they are trusted when using business resources and equipment.

- ➔ Employees are allowed privacy of confidential and personal information.

Employers have the right to monitor traffic and activities on ICT systems, however, they must respect the privacy of confidential and personal information.

Employer's monitoring of work emails, internet access and computer use:

To summarize, employers have the right to monitor ICT systems as they have the right to:

- ➔ Provide legal protection over the business.
- ➔ Ensure business standards are upheld and a positive image is reinforced.
- ➔ make sure their workers are working productively.
- ➔ Protect ICT systems from malware and other security breaches that could compromise the business and its information.

However,

Employers must consider employee's rights to:

- ➔ Have a sense of trust – the employer-employee relationship should be transparent and filled with trust.
- ➔ Take regular breaks to ensure they can stay healthy and function efficiently.
- ➔ Have their data protected and safety knowing that their information won't be shared with others – confidentiality.

Note**: there is always a legal and moral conflict between the rights for employers to monitor employee privacy because of the sensitive nature of this topic.

Online censorship of information in a global context

Online Censorship:

Online censorship refers to the controlling of information that is allowed to be accessed and published by users on the Internet.

- ➔ The scale at which censorship occurs varies.
  - It can come in the form of web filters in a school to maintain productivity.
  - It can also resemble the grandiose Great Firewall of China which prohibits all inhabitants in China from accessing websites such as Facebook.

Online Censorship in an Australian Context:

Australia currently has no online censorship on the grounds of religious and political freedom being pivotal to the functioning of the nation – we endorse freedom of speech.

- ➔ In June 2015, the Copyright Amendment Bill 2015 allowed courts to block websites that are known to cause copyright infringement hosting and distributing content illegally.

Online Censorship in a Government Context:

"The free flow of information is essential to Internet freedom. Internet freedom is online freedom of expression in the 21st century and enables the dissemination of information and ideas that are the building blocks of economic growth and democracy. Filtering or regulation by governments or private Internet access providers curtails the democratizing effects and economic benefits of the Internet."

- ➔ Without censorship, governments would be able to easily manage:
  - Violations of human rights,
  - Surveillance,
  - Free trade.
- ➔ Government-to-government diplomatic engagement including multilateral efforts and social media engagement across diverse cultures are key to combating state-sponsored online abuses that are on the rise.
  - This includes blog infiltrators,
  - Technical and physical attacks on citizens for their online speech,
  - Hijacking of personal accounts,
  - Pressure on intermediaries leading to voluntary takedowns of content.

Impacts of Online Censorship:

- ➔ It halts the flow of information between parties.
  - whilst fake information can be restricted, so can real information – it is very difficult to sift through the onslaught of data packets that travel the globe each day.
- ➔ Provides a negative economic impact.
  - If a business has their website blocked because it doesn't meet the arbitrary standard of "good", then they won't be able to sell their goods on an e-commerce platform or promote themselves.
    - They would be disadvantaged compared to industry competitors who are allowed to sell online.
- ➔ Inhibits freedom of speech.
  - A free internet allows individuals to post what they want. Laws already exist that punish those who share illegal content such as child pornography.
    - Why compound the limitations of thoughts and opinions and add another layer of bureaucracy to the internet that isn't needed?
- ➔ A lack of truth leads to ignorance.
  - Societal ignorance as a direct consequence of a lack of truth allows a specific group to be able to seize control.
- ➔ Limits entrepreneurial opportunities.
  - Censorship implies that an overseeing body reviews everyone's information, including those seeking to be creative and innovative.
    - This can result in government repression of ideas and puts the originality of their idea in jeopardy when it is scrutinized by other bodies.

Put simply:

- ➔ Increased workplace productivity via removal of distractions.
- ➔ Decreased diversity of political and religious views.
- ➔ Increased in loophole websites that bypass censorship being present on the Web.
- ➔ Reduced security risks (e.g. reduction in accessibility of terrorism websites)

Issues with the use of cloud computing:

Confidentiality of data:

When data is saved in the cloud, it is at the whim of the cloud service provider (CSP).

- ➔ When the data is saved on a personal device, the data is relatively safe, however, once cloud storage is employed, its safety is endangered.
  - Hackers may be able to access a cloud service provider's many clients and their data, compromising business secrets and the like.
    - The question to ask is whether where you are saving your data is secure of not, and whether it is the storage solution you need.
- ➔ By uploading your data to a CSP, you are surrendering control of it.
  - You no longer have control over security, ownership/IP and privacy of it.
    - Ask yourself:
      - What are the privacy policies of the CSP?
      - What are the privacy laws?

Sensitivity of documents:

Whilst all data stored in the cloud is important, some are more important than others.

- ➔ Trade secrets would be prioritized over school documents.
- ➔ Patient records for hospital systems are also sensitive and should be stored aside from blog content etc.
  - The more sensitive the document, the more care needed to keep that document safe.

Level of accessibility:

Accessibility to content on the web varies:

- ➔ Some information requires a login to get information.
- ➔ How can it be accessed, website?

Availability of online applications

The more applications that exist, the more online data we have.

- ➔ We can use online applications such as social networking to keep in touch with family and friends.

Conversely, the more data that is stored online, the more opportunity for criminal activity such as theft and fraud.

Impact of digital technologies and global markets on:

Productivity:

Consensus on Productivity:

Global markets provide more opportunities for consumers to pick and choose their purchases; there is a greater variety of products available in the consumer marketplace.

- ➔ Examples of this include:
  - Apple's global productivity has significantly increased as a result of digital technologies. iPhone sales are exponentially increasing.
  - Improvements to the online learning space alleviates the pressure of needing university professors and other scholars to educate the masses.
  - Improvements in medical diagnosis equipment in the form of MRI for example, allows the doctor's decisions and analysis to be more detailed and conclusive – eliminating doubt.

The Impact of Global markets on Productivity:

Digital convergence plays a massive part in that companies can produce highly commercially successful products that can cater for differing markets around the world.

- ➔ An example of this would be the iPhone in that it is customized for any market and thousands of applications – it is not geo-restrictive.

Improvements in communication technology allows for real-time access to production and machinery and remotely from anywhere in the world; this allows for mining, transport and manufacture etc. to be done remotely.

- ➔ This is echoed in a variety of fields such as forensics etc.

The Impact of ICT on Education:

ICT is a means to which the accessibility and efficiency of education in many countries.

- ➔ ICT can also be viewed as a enabler for the masses by providing access to the latest educational content around the world.
  - However, there is still a significant digital divide between educational institutions located in developing and developed countries
    - This includes policy and infrastructure gaps, lack of training facilities and personnel, ICT access issues, etc.

Advantages (ICT systems):

- ➔ Reduces costs.
  - Eliminates costs incurred from automation or reducing material costs such as printing paper.
- ➔ Increased flexibility.
  - Allows users to work in a dynamic work environment; they are able to access business content on the go with ease, eliminating lost productivity brought about by transportation or their environment.
- ➔ Increased capability.
  - Can provide virtual communication between managers and staff.

- Essentially, provides businesses a geographical communication advantage as they are no longer constrained by their location, so long as they have an Internet connection, they can communicate.

Disadvantages (ICT systems):

➔ Increased employee distractions.
- ICT enables users to have easier access to distracting material.
  - The portability of digital devices intensifies this effect, in that it is even easier to access distracting content on phones, on-the-go now.

➔ Greater employee vulnerability to advertising.
- Systems can track a user's personality characteristics and interests and feed them content that appeals to this, further distracting them and leading to a loss in productivity.

➔ Greater dependency on ICT systems.
- Failure of an ICT system could lead to a loss in productivity.
  - Internet-reliant business would suffer if the Internet went done.

Access to knowledge or resources:

Consensus on Access to Knowledge or Resources:

The presence of digital technologies and the Internet allows for 24/7 access to:

➔ University and online courses = cheaper method of getting a degree.
➔ Scholarly sources and articles = enrichened and enlightened populace.
➔ Movies on demand = eliminates transportation for entertainment.
➔ Games = allows for diverse hobbies.
➔ Cloud storage = convenient means of storage, but is the security compromise worth it?
➔ Emails and co. = allows on-the-go access to emails and the like.
➔ Social networking = constant updates on current affairs and is a means of constant communication with others across the globe.
➔ Cyberbullying = a more prevalent theme as the Internet evolves.

Outsourcing:

Outsourcing is 'offloading' of production or a service to another company to complete instead.

➔ Outsourcing means that the product or service that is provided is in fact owned by another company or individual.
- Local outsourcing = means provided within the state or country.
- Global outsourcing = means provided by another country on the globe.

Impact of Web 2.0/Web 3.0 on the use of digital technologies

The Web 1.0 was about web connectivity;

➔ This came in the form of AOL, Yahoo and Google.

Web 2.0 was social with Facebook, LinkedIn as the foundational creators of the web's 'social layer'.

➔ Web 2.0 is the current version of the web that focuses on sharing of information and virtual collaboration. It revolves around:

- Dynamic user interfaces, evolved from static user interfaces of Web 1.0
- Emergence of social networking and other virtual collaboration tools.
- Finding information more easily with more developed and faster search engines.

With Web 3.0 we are more looking into virtual world being created through the web such as online virtual shopping malls and tradeshows. Essentially, the Web 3.0 is the future version of the web that focuses on:

➔ Web 3.0 is all about personalization and the Sementic Web while integrating real-time data through different platforms. Semantic technology will create a meaningful format around human interaction online and human interests.
➔ Eventually, as our devices learn more about our preferences. We can simply as a question, and we will get a response tailored to your interests.
- Greater connectivity between internet enabled devices – development of the internet of things where ordinary household devices will be able to communicate wirelessly.
- Internet searches based on a user's own internet rather than keywords.
- Intelligent processing of information with web technologies learning from past user activity.
- Faster and more complex online applications.

MANAGING DATA

Security Techniques for the Management of Data:

Disaster Recovery Plan:

A disaster recovery plan is a written plan that describes the steps an organization would take to restore its computer operations in the event of a disaster.

➔ A disaster can be natural or man-made (hackers, viruses, etc.)
- Each company and each department or division within an organization usually has its own disaster recovery plan.

Disaster Recovery Plan Steps:

➔ Emergency plan = specifies the steps a company will take as soon as a disaster strikes. The emergency plan is organized by type of disaster.

It should include:

- Name and phone numbers of people and organization to notify e.g. police.
- Computer equipment procedures, such as equipment or power shutoff, and file removal.
  - These procedures should be followed only if it is safe for an employee to do so.
- Employee evacuation procedures.
- Return procedures; who can enter the facility and what they should do.

➔ Backup plan = specifies how a company will use backup files and equipment to resume computer operations.

This includes:

- The location of backup data, equipment and supplies.
- Who should be responsible for gathering backup resources and transporting them to an alternate computer facility.
- The method that data t backed up on cloud storage will be restored by.
- A schedule indicating the order and approx. time each application should be up and running.

➔ Recovery plan = specifies the actions a company will take to restore full computer operations. This differs depending on the disaster.
- Different groups should be responsible for different forms of recovery, such as replacing hardware or software.

➔ Test plan = includes simulating various levels of disasters and testing the company's ability to recover.
- This should uncover flaws in the recovery plan, so that it can be finetuned and safe.
  - This should happen frequently and without the participants knowing, to better simulate a disaster.

Considerations for Disaster Recovery:

➔ Natural Disasters = for natural disasters, the following should be done:

Shut off power, evacuate, if necessary, pay attention to advisories, do not use telephone lines if lightning occurs.

➔ What Might Occur:

Power outage, phone lines down, structural damage to building, road closings, transportation interruptions, flooding, equipment damage.

➔ What to Include in the Plan:

Satellite phone, list of employee phone numbers, alternate worksites, action to be taken if employees are not able to come to work/leave the office, wet/dry vacuums, make and model numbers and vendor information to get replacements.

Audit Trail:

Audit trails are an electronic/ paper log that records specific details relating to a user's access to a file.

➔ This includes but isn't limited to: when the data was accessed, who accessed it, what was accessed.
  - Audit trails give administrators the ability to monitor the accessing and modification of data and to identify unusual behavior to be investigated further.
    - Changes made to files etc. can be linked to specific users, allowing the administrator to easily find data tamperers.

Types of Backup Techniques and Archiving of Data:

Full:

A full backup makes a copy of the entire contents of a system onto an external source.

- ➔ Advantages:
  - Fastest recovery method available.
  - All files are saved; eliminating the chance of something being missed by the backup.
- ➔ Disadvantages:
  - Longest backup time.
  - Uses a large volume of storage space.

Differential:

A backup that makes a copy of all new or modified files since the last full backup.

- ➔ Advantages:
  - Fast backup method.
  - Requires minimal storage space to back up.

- ➔ Disadvantages:
  - Backup files are scattered amongst multiple locations.
  - Recovery is time consuming because the last full backup and differential backup are needed.

Incremental:

A backup that makes a copy of all new or modified files since the last full backup or incremental backup.

- ➔ Advantages:
  - Requires minimal storage space to back up.
  - Only most recent changes saved.
  - Fastest backup method.
- ➔ Disadvantages:
  - Recovery is the most time-consuming because the last full backup and all incremental backups since the last full backup are needed.
  - Backup files are scattered amongst multiple locations.

Daily:

A backup that makes a copy of all new or modified files on the day of the backup. These are performed daily.

- ➔ Advantages:
  - Uses least amount of space.
  - Shortest backup time.
  - Regular backing up of files.
- ➔ Disadvantages:
  - Backup files are scattered amongst multiple locations.

Online Data Storage Methods:

Data Warehouses:

Data warehouses are facilities that hold and contain all data for a business.

- ➔ They are comprised of hundreds of servers connected to provide users their specific data.
- ➔ It also provides the business a summary of their historical transaction data.

Data Marts:

Data marts are a subsection of a data warehouse that holds data relating to a specific function or department of a business.

Data in the Cloud:

Data in the cloud refers to online cloud storage, where data is stored offsite of business premises; the data is present on internet connected servers located around the world.

- ➔ Security and privacy of the data is surrendered to the cloud storage provider.
  - Their license agreements outline what the CSP can do with your data.
    - In addition, data stored around the world is subject to different privacy laws.

Purpose of Data Mining:

Data mining is the extracting of patterns, trends or information from a set of data.

- ➔ Majority of the things you can do online can be appropriated for data analytical purposes, such as:
  - Search engine queries – recording recent internet searches.
  - Cookies.
  - Social media activity – voluntary information given when creating a profile.
  - Internet tracking software.
  - Online purchasing history.
- ➔ Offline means of data collection includes:
  - Credit card transactions.
  - Loyalty cards – e.g. Flybuys, Myer One.
  - Survey or competitions.

Marketing Purposes:

The primary purpose of data mining is for marketing purposes.

- ➔ This information is collected to build a profile about a user.
  - This comes in the form of name, sex, interests and location etc.
    - This is due to the fact that once marketers know their target audience and their characteristics, they can better promote products based on their interests and attributes.
      - Algorithms are used to detect and identify certain online trends to build a customer profile.

Medical/Scientific Purposes:

Data mining can be used to link symptoms together to identify an illness.

- ➔ For example, if you have a high temperature and running nose, you could get diagnosed as having a fever.
  - Web MD uses voluntary inputted data from its online forms to determine possible illnesses.

Security Purposes:

Business can use data mining by analyzing the activities of its employees and detecting any unusual activity.

- ➔ For example, suspicious would be raised if a junior employee accessed sensitive files, used only by senior employees.
  - In a wider context, data mining can be used to detect suspicious activity.

Processing of Data Considering Security of Data through the Use of Passwords:

Passwords:

A combination of characters linked to a username which unlocks access to certain computer resources.

Firewalls:

A hardware, software or router, that checks the incoming and outgoing data packets of a network and rejects any unauthorized data packets entering or leaving the network.

Biometrics:

Unique human characteristics used to verify the user to unlock access to certain computer resources. This includes:

- ➔ Fingerprints, eyeball, voice, facial recognition.

Anti-virus Software:

Software installed on a device with the purpose of monitoring and removing malware. Malware is checked against a list of regularly updated virus definitions.

Digital Signatures:

An electronic code, embedded in a document via public key infrastructure, with the purpose of verifying the contents of the document and the sender's identity.

Digital Certificates:

An electronic passport that uses public key infrastructure to secure and transmit data between a website and a user's device.

Encryption:

The process of encoding data, through algorithms, so it can only be read by the sender and its intended recipient.

➔ Encryption uses public key infrastructure, which consists of two keys, a public key that anyone can obtain off the web, and a private key known only by the sender and the intended recipient.

Concept of user-generated content:

User generated content (UGC) is where voluntary contributors can publish online content. Examples of this includes:

➔ Wikipedia.
➔ Social Networks – Facebook, Twitter, YouTube.
➔ Forums – Whirlpool, Reddit.
➔ Review Websites – Zomato.
➔ Online classifieds – Gumtree.

Advantages and disadvantages of user generated content:

Benefits of User Generated Content for a Website Owner:

➔ Free = the website owner does not have to fork out wages to staff to produce content.
➔ Provides feedback = general user opinions can be viewed as valuable towards feedback and decision making.
- For example, checking the rating of a restaurant before deciding where to eat.

➔ Self-policing opportunities = forums can be monitored by voluntary moderators.
➔ Keeps users engaged = users often participate with discussions with one another, keeping users engaged and increasing the number of returned users.

Costs of User Generated Content for a Website Owner:

➔ Bias = users often hold strong opinions about a topic and oten don't contribute a balanced perspective.
➔ Lack of reliability and credibility – anyone can publish content – there is no guarantee that information presented in user generated content is factual.
- This is why Wikipedia has a poor reputation and often avoided in referencing.

➔ Online defamation risk = users can publish false, offensive or inappropriate content that could pose a legal liability towards the website owner.
➔ Confusion over Intellectual Property = who owns user generated content?

Concept of hypertext markup language:

Hypertext Markup Language is a markup language used for the structuring and presentation of websites. HTML consists of plain text and HTML tags.

➔ HTML is the standard for the Web as established by the W3C.
- HTML 5 is the current version of HTML and allows for:
  - Multimedia support = live streaming.
  - Interactive elements.
  - Additional Online Form Validators = field and range checks.
    - HTML 5 advancements means old browsers are no longer compatible.

Concept of Web 2.0 and Web 3.0:

Web 2.0:

Web 2.0 is the current version of the web that focuses on the sharing of information and virtual collaboration. It revolves around:

- ➔ Evolution of dynamic user interfaces from Web 1.0. static user interfaces.
- ➔ Emergence of social networking and other virtual collaboration tools.
- ➔ Finding information more easily with more developed and faster search engines.

Encryption:

Web 3.0 is all about personalization and the Semantic Web while integrating real-time data through different platforms. Semantic technology will create a meaningful format around human interaction online and human interests.

- ➔ Eventually, as our devices learn more about our preferences, we can simply ask a question, and we will get a response tailored to our interests.

Purpose and features of content management systems (CMS):

A CMS is an online publishing tool that allows users to create, edit and publish online content without the use of development tools or knowledge of HTML.

- ➔ Examples include WordPress and Blogger.

Features of a Content Management System:

- ➔ User-friendly interface.
- ➔ Security features.
- ➔ Social networking integration (ability to share posts on social media).
- ➔ Possible collaborative features – allowing multiple editors for one document.

Purpose of world wide web consortium (W3C):

The W3C are an international community where member organizations, full-time staff, and the public work together to develop Web standards.

- ➔ The development of web standards ensure the singular evolution of the web rather than it being split into multiple directions by groups.
  - Ultimately, their mission is to lead the Web to its full potential.

Purpose of W3C conventions:

Web standards are a set of rules that web developers should follow when developing and choosing file formats for their websites.

- ➔ These rules guide developers in ensuring accessibility and compatibility for all users. Examples of these include:
  - PNG for raster graphics and SVG for vector graphics.
  - HTML for markup languages and CSS for the design of a website.
  - Accessibility, usability and inclusivity standards.

Purpose of the Web Design and Applications standard from the W3C standards, including:

HTML and CSS:

HTML and CSS are the fundamental technologies for building web pages.

- ➔ HTML = structure.
- ➔ CSS = style and layout.

Graphics:

W3C is the home of the widely deployed PNG raster format, SVG vector format, and the Canvas API.

- ➔ Graphics are used as a visual representation on Web sites to embody concepts or feelings to better reach users.
  - Standards are put in place for this to express artistic creativity, data visualization and optimizes the presentation of information.
    - WebCGM is a more specialized format, in fields such as aeronautics.

Audio and video:

Some of the W3C formats that enable authoring audio and video presentations include HTML, SVG and SMIL.

- ➔ W3C is also working on a timed text format for captioning and other applications.

Accessibility:

W3C's Web Accessibility Initiative has published Web Content Accessibility Guidelines (WCAG) to help authors create content that is accessible to people with disabilities.

- ➔ WAI-ARIA gives authors more tools to create accessible Web Applications by providing additional semantics about widgets and behaviours.

Internationalization:

W3C has a mission to design technology that works across cultures and languages.

- ➔ W3C standards such as HTML and XML, are built on Unicode for instance.
  - W3C has also published guidance for authors related to language tags bi-directional text, and more.

Mobile Web:

W3C promotes "One-Web" that is available on any device.

- ➔ W3C's Mobile Web Best Practices help authors understand how to create content that provides a reasonable experience on a wide variety of devices, contexts and locations.

Validation techniques for online forms:

Validation techniques are methods to ensure that data entered on online forms are correct and up-to-date.

- ➔ Validation techniques are important because data is valuable to organizations and incorrect data is useless.
  - There are organizations in Australia with the main purposes of collecting and selling data for marketing purposes.

Examples of this include:

- ➔ Range check = checks that numbers entered are within a defined range.
- ➔ Field check = checks that all required fields have been entered.
- ➔ Length check = checks that the entered fields don't exceed a defined limit, such as a character limit or word limit.
- ➔ Email verification = checks the entered email address is legitimate.
- ➔ CAPTCHA = checks that the person entering the online form is a human and not a robot.