1. Peruse the [Australian Privacy Principles](https://www.oaic.gov.au/privacy/australian-privacy-principles/) page and [Australian Privacy Principles quick reference](https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference/) page:

|  |
| --- |
| APP 1. Open and transparent management of personal information |
| APP 2. Anonymity and pseudonymity |
| APP 3. Collection of solicited personal information |
| APP 4. Dealing with unsolicited personal information |
| APP 5. Notification of the collection of personal information |
| APP 6. Use or disclosure of personal information |
| APP 7. Direct marketing |
| APP 8. Cross-border disclosure of personal information |
| APP 9. Adoption, use or disclosure of government related identifiers |
| APP 10. Quality of personal information |
| APP 11. Security of personal information |
| APP 12. Access to personal information |
| APP 13. Correction of personal information |

Explain (giving examples) how these principles may impact the ethical use or management of student data in a school information management system. Your answer must not be longer than half an A4 page. Answer in dot points, indicating which principle you are referring to, and which action or impact the school may have, for example:

* APP 7: The school may advertise a musical to its parents, but parents must have the option to “opt out” of receiving the advertisements

1. Read the following definitions then answer the question at the bottom of the page. You are welcome to use the internet for more research:

|  |  |
| --- | --- |
| Definition | Explanation |
| latency | Latency (aka 'ping', 'ping rate' or 'delay') is the amount of **delay** (milliseconds / ms) between a user action and the resulting response. High latency = high ping = high 'lag' (when gaming): |
| jitter | Jitter (aka 'ping spikes' or 'stuttering') is the fluctuation or variation of *latency* **over time**. Jitter is also measured in ms, and is calculated by finding the difference between a sample of *latencies* **over time**.  Jitter can be caused by queuing, buffering, processing loads, and competing traffic (for a resource).  Too much jitter can result in *packet* loss, due to packets not arriving in the same order they were sent. Jitter “buffers” can protect against this, but if these buffers overflow then a user will experience *jitter induced packet loss*. |
| bandwidth | Bandwidth is the term used for the **maximum** transfer capacity of a network |
| throughput | Throughput is the (actual) amount of data that can be sent and received within a specific timeframe. It can be limited by packet loss, latency, enforced limitations, congestion, protocols being used, and other factors. |

**Question**: A customer is having difficulty using his Skype video call software in the evening. His laptop is brand new and up to date, and his home internet devices have been correctly installed, configured and updated. Still, he receives **poorer quality video and sound connection at peak time**, despite being on a data limited 40mbps bandwidth plan. Explain to the customer in simple terms using at least the *jitter* and *latency* defintions as to why his call quality may be poor. Your answer must not **exceed** 3 paragraphs in length (12 sentences maximum).

1. Read about the following protocols then add to the list using your own internet research **FTP** (File Transfer Protocol):

|  |  |
| --- | --- |
| Protocol (set of rules) | Explanation |
| ip | **Internet Protocol**, which attaches address information to every packet of data sent so that internet routers can locate a packets intended destination. Every device or domain connected to the internet has an **Internet Protocol** (IP) address, and each IP packet will contain both sender and recipient IP address. |
| tcp | **Transmission Control Protocol**, a method through which packets of data are compiled that *guarantees* a reliable communication channel over an unreliable network (i.e. when packets are lost from congestion or arrive out of order).  TCP:   * determines how to break application data into packets that networks can deliver * sends packets to – and accepts packets from – the [*network layer*](https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.halc001/ipcicint_protocol.htm) (where IP operates) * manages flow control – so if a receiver is being ‘overwhelmed’ with packets, TCP will adjust (stop temp or buffer) * handles retransmission of dropped or garbled packets, and acknowledges all packets that arrive to provide *error-free data transmission* (see highlighted paragraph below) * can adapt to the *delay* characteristics of a network and adjust its operation to maximize *throughput* without overloading the network   TCP guarantees the recipient will receive the packets in order by numbering them. The recipient sends messages back to the sender saying it received the messages. If the sender does not get a correct response, it will resend the packets to ensure the recipient received them. Packets are also checked for errors. TCP is all about this reliability – packets sent with TCP are tracked so no data is lost or corrupted in transit. |
| udp | **User Datagram Protocol** is like TCP but **without error checking**. Packets are continually sent to the recipient without waiting to make sure a recipient received the packet. If a recipient misses UDP packets, they are just lost – there is no way to re-request them, or to guarantee that all packets sent have been received. This makes UDP communication a lot quicker than TCP, and is useful when lost packets of data doesn’t really matter, but speed of delivery does – such as during video streaming or gaming. |
| http | Hypertext Transfer Protocol is an *application protocol* (which means it operates at the [application layer](https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.halc001/ipcicint_protocol.htm)) used for transferring hypermedia (such as web page files in a browser). It is a stateless protocol in which a connection is established via TCP between client and server (typically on port 80). Some HTTP methods used in IA2 and IA3 include GET and POST. HTTP also delivers response codes you may have seen e.g. 500 internal server error, 404 not found, 200 ok, etc. 5XX are server errors, 4XX client. |
| https | Extension of HTTP but the s stands for secure. The security is an encryption layer provided by [Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security) (formerly SSL) at the transport layer, and typically connects on port 443. TLS (aka SSL) uses both asymmetric (establishing the client-server ‘session’) and symmetric (when exchanging data) encryption. This means that anything after the https://www.voidinit.com/this/is/hidden/from/isp/in/TLS is hidden from ISP, as is POST / GET msgs |

1. Masking your own devices IP address to stay anonymous is possible through the use of:

|  |  |
| --- | --- |
| Technology | Explanation |
| vpn | *Virtual Private Network*, allows you to connect to a remote server at the OS level (so can work for all apps), and use that servers internet connection to browse the web. This connection creates an ‘encrypted data tunnel’ between client and VPN, which hides browsing history from ISP, and IP address / location from servers where a response is requested. |
| proxy | Proxy servers are similar to VPNs in that you can connect to a proxy server, and browse the web from there, and both will keep you anonymous / unidentified at the hardware level from the outside world (although neither will protect you from any information you choose to give out at the application level) – which is pretty much what happens in most State / Catholic schools in Queensland. Proxy servers can also cache pages and are often used to filter (given where they are used).  The difference with proxies (as opposed to VPNs) is that proxies work at the application level (you have to set them up for each different application you are using, e.g. Chrome) and proxies won’t encrypt your traffic (so will be slightly quicker). |
| onion routing | A technique where a message is sent through multiple routers (nodes), where each node knows the previous and next node location in the chain, but not whether the previous or next node is the origin or destination. Each time a request is bounced a layer of encryption is ‘peeled’ back to reveal the next destination node (hence onion). This is achieved through asymmetric encryption. By ‘bouncing’ traffic through these nodes, the requested server response cannot see the origin client location or IP address, only the most recent node making the request. This is anonymous but **very** **slow** compared to accessing the same HTTP sites via direct connection, given the extra routing that takes place.  The network that performs onion routing is known as an onion network (the network is known as the “The Onion Router”, or TOR), and sites hosted on the onion network have the TLD .onion. These sites are not indexed with a DNS and many are *difficult* to find / not indexed / searchable.. the most hidden sites (depending on the illegality of them) are referred to as the “dark” or “deep” web.  There isn’t a single valid reason for an Australian school student to have a Tor browser installed on their laptop, which is why using a browser that is capable of navigating these sites invites people to question your intentions for having these browsers installed (such as the Tor Browser) and thus land you in **trouble** simply for having the software installed. |

**Question**: Using the knowledge from all of the previous questions you have gained so far, write 3 technical recommendations for Queensland Health to implement *safe* and *secure* internet access for its employees.

Use knowledge gained above, or your own internet research, to discover:

1. How is [broadcasting](https://en.wikipedia.org/wiki/Broadcasting_(networking)) different from [multicasting](https://en.wikipedia.org/wiki/Multicast) on a computer network?
2. Why is media (audio or video) streaming better with UDP (as opposed to TCP)?
3. How can buffering benefit streaming?
4. Explain how these factors impact a stream:

|  |  |
| --- | --- |
| Latency |  |
| Jitter |  |
| Bandwidth |  |
| Throughput |  |