Your response

Zero-rating

Question	Your response
Question 1: Do you agree with our assessment of zero-rating offers and our proposed approach?	Confidential? – N Yes, in general it seems reasonable and proportionate.
Question 2: Do you agree with the criteria we use to define Type One, Type Two and Type Three zero-rating offers and our proposed approach to such offers?	Broadly yes, but Type 1 could be expanded to include information services or providers endorsed or contracted by public sector – eg certain charities & healthcare bodies, or perhaps providers of educational services such as examination boards. There also needs to be more thought given to what happens if government agencies use cloud-based platforms or software functions, eg if they are based on AWS or Azure, or use 3rd-party cloud-based services such as identity-verification or medical image diagnostics inside a tax or medical application.
Question 3: Do you agree with the approach in our guidance in Annex 5 in relation to zero-rating?	It will be very difficult to define "classes" of similar applications, especially as many apps are multi-function. (eg a live-stream or game or financial function within a social network, or a messaging function inside a business or travel application) As with Q2, there is also an issue of how cloud-based software elements are classified if they are used within an app, or based on a 3rd-party site or platform such as AWS or delivered from a CDN. Lastly, it is unclear how any of this may deal with users or devices that connect via a VPN or other form of encrypted or proxy'd path. There should also be clarity about any different

	treatment of CAPs accessed via a browser or web-app, rather than a "native" app. There also needs to be some right for users to complain about problems with zero-rated services.
Question 4: What are your views on whether zero-rated content should be able to be accessed once a customer's data allowance has been used up?	This seems OK, unless the volumes accessed under zero-rating exceed a certain % or multiple of the underlying data allowance. it would seem unreasonable to stream 10GB of zero-rated videos, after a 1GB allowance was consumed, and could be a workaround enabling anti-competitive models.
Please provide any further evidence you have to support your responses.	

Traffic management

Question	Your response
Question 5: Do you agree with our assessment of retail offers with different quality levels and our proposed approach?	Confidential? – N Yes, the assessment seems reasonable
Question 6: Do you agree with the approach in our guidance in Annex 5 in relation to differentiated retail offers, including transparency requirements, improved regulatory monitoring and reporting of retail offers with different quality levels as well as the general quality of the internet access services?	Broadly agree There needs to be clarity on issues such as: - Any difference in treatment of uplink and downlink traffic - Responsibility of the ISP in situations where quality cannot be maintained (eg areas without good mobile coverage) & any recourse the user has in such situations, for instance if the indoor of their home has poor signal. - Transparency should be made available in more detail for application developers or device suppliers, which may be more able to describe impacts on quality-of-experience for a specific application or service, or in specific situations - There needs to be detail on how ISPs may deal with users or devices that connect via a VPN or other form of

	encrypted or proxy'd path. There should also be clarity about any different treatment of CAPs accessed via a browser or web-app, rather than a "native" app. Ofcom should consider any extra cybersecurity and privacy risks of excluding users / devices with VPNs
Question 7: What are your views on a more permissive approach towards retail offers where different quality levels are content and service specific?	This has significant risks for the future health of the public Internet & its ecosystem There is an argument for specialised services that are genuinely "special", but there needs to be clear justification of this. It will be very difficult to define "classes" of services or similar applications, especially as many apps are multi-function. (eg a live-stream or game or financial function within a social network, or a messaging function inside a business or travel application) As with Q2, there is also an issue of how cloud-based software elements and services are classified if they are used within an app, or based on a 3rd-party site or platform such as AWS or delivered from a CDN. Meanwhile, there should be a move away from the term "best efforts" to a new regime called "good enough", which would evolve to meet the reasonable expectations of "non-special" services over time.
Question 8: Do you agree with our assessment of how traffic management can be used to address congestion and our proposed approach?	No comment
Question 9: Do you agree with the approach in our guidance in Annex 5 in relation to the use of traffic management to address congestion, including transparency requirements, improved regulatory monitoring and reporting of general network performance metrics, the use of traffic management and the impact on service quality?	ISPs should make available some form of "congestion APIs" or other information mechanisms allowing users, devices and application developers to make intelligent assessments of network conditions, both in near real-time and with historical expectations Oversimplified, but this could manifest as something akin to: "There is currently a spike in demand & imminent congestion. We suggest downrating

	video resolution for the next 20mins” “There is often network congestion in the vicinity of Oxford Circus at 5pm on Saturdays, and on Wembley Way an hour before kick-off”
Question 10: What are your views on a more focused approach to traffic management to address congestion?	No comment
Please provide any further evidence you have to support your responses.	

Specialised services

Question	Your response
Question 11: Do you agree with our assessment of specialised services and our proposed approach?	Confidential? – N Broadly agree. There should be explicit recognition that: - There is almost zero public demand from CAPs for “fast lanes” or other similar capabilities, despite the idea being widely discussed for at least 10-15 years. Has Ofcom ever received responses from CAPs specifically requesting such capabilities be made available? (There may be some exceptions for industrial / enterprise applications) - As before, there needs to be clarity about the roles of different participants, for instance where CAPs use hyperscale cloud platforms or CDNs, or where 3rd-party software elements are parts of a given service or application. - There needs to be clarity on the cost implications of user-generated traffic, eg if someone uploads a TB of data, streams video 24x7 from a camera, or emails large files to their whole address book. Is the CAP responsible for all uploads & incurred costs? - There is no obvious demand from ISPs’ own content/application businesses for such services when used on *other* ISP networks. They also do not appear to have requested priority for their (premium, paying) roaming customers

	on other networks when visiting. They appear only to be interested in selling QoS, not buying it. Given their deep knowledge & understanding of the matter, it seems strange that they don’t want to “eat their own dog food” - Potentially, providers of specialised services should not be permitted to use the word “Internet” to describe the offers. Maybe “Ain’ternet” would be more appropriate? - There needs to be more consideration given to “two stage” connectivity, such as where there is in-building managed Wi-Fi, or a 3rd party neutral host in the traffic path. What are their responsibilities? Is an ISP-managed WiFi mesh part of the access network, or can that be used to create non-neutral services outside the rules? If the user is in control (eg prioritising WFH traffic over childrens’ games on the home WiFi) how is that dealt with in Ofcom’s proposals? - There should be some guidance on “hybrid” public/private networks, either where a private network offers secondary access to public providers (eg as a neutral host in a factory), or where public mobile networks have an “extra tenant” of a private network in certain locations.
Question 12: Do you agree with the approach in our guidance in Annex 5 in relation to specialised services, including transparency requirements, improved regulatory monitoring and reporting of the need for optimisation of a service, the general performance of internet access services and the impact of specialised services on the quality internet access?	There needs to be detail on how ISPs offering specialised services may deal with users or devices that connect via a VPN or other form of encrypted or proxy’d path, or alternative DNS. There should also be clarity about any different treatment of CAPs accessed via a browser or web-app, rather than a “native” app. Ofcom should consider any extra cybersecurity and privacy risks of excluding users / devices with VPNs There should be clarity on specialised services delivered in conjunction with specialised networks, for instance additional 5G radio coverage installed at a factory, or upgrades to cover a farm or port or other outdoor area and

	so on. If such equipment / upgrades would not normally have been installed for general Internet access, it seems unreasonable to mandate the same lack of impact on general Internet access as in normal “public” network contexts.
Please provide any further evidence you have to support your responses.	

Scope of the net neutrality rules, terminal equipment and public interest exceptions

Question	Your response
Question 13: Do you agree with our assessment of the terminal equipment rules and our proposed approach?	Confidential? – N Yes, although there is insufficient detail about the use of some terminal equipment (such as WiFi routers / gateways / meshes and settop boxes) that could themselves implement traffic management or prioritisation mechanisms. Where these are provided and managed by the ISP (perhaps with a 3rd party cloud management capability) there needs to be clarity on where the scope of the Neutrality rules & guidelines reach and how transparency should be conducted. These same on-premise devices such as WiFi gateways could also be used to restrict Internet access from known compromised IoT devices or other sources of malware.
Question 14: Do you agree with our assessment of internet access services provided on aeroplanes, trains, buses and coaches and our proposed approach?	There should be some specific discussion of “semi-public” connectivity providers, such as WiFi at train stations, or inside large multi-dwelling units without ISP choice. With regard to traffic management, some on-train WiFi systems block certain forms of content such as video or applications such as VPNs. This is ostensibly intended to address congestion, but sometimes more reflects unsophisticated traffic management techniques and/or a desire to force users via some sort of captive portal & data analytics “monetisation” system. Given that business travellers in particular may want to use videoconferencing

	or encryption, this seems to be unacceptable traffic management. Given government policy to encourage more travel on public transport rather than road, VPN blocks in particular seem to be counter-productive as well as creating greater cybersecurity vulnerabilities. It should be noted that many enterprise-issued laptops are “locked down” with security features that may limit their use on networks deemed insecure.
Question 15: Do you agree with our proposed approach to emergency 999 communications services and that we should consider amending the GCs to achieve this?	No comment
Question 16: Do you agree that ISPs should be allowed to block scams and fraudulent content and provide in-network parental controls and content filters?	Yes It is worth noting that some networks (including in-home Wi-Fi systems) could act as cybersecurity enforcers where certain classes of end-device are compromised (eg IoT products determined to be a risk)
Please provide any further evidence you have to support your responses.	