GUIDELINES FOR OFFER SUMMARY

TRAFFIC MANAGEMENT AND SERVICE RESTRICTION DEFINITIONS

September 2016

1. INTRODUCTION

1.1. The guiding principles which underpins industry best practice for Traffic Management outlined in this document is to provide end users with transparent information on how an RSP discriminates, restricts or interferes with their traffic, on the basis of commercial rivalry and/or discrimination against another content provider or network operator.

2. PURPOSE OF THIS DOCUMENT

2.1. This document is guidance for the interpretation of the Traffic Management section in the TCF Product Disclosure Code of Practice ('Code') and outlines what should be added to the Offer Summary for 'service restrictions', specifically it:

- Defines Traffic Management and describes what will be included in the Code for the Offer Summary Traffic Management section
- Outlines what will be included in the Offer Summary for service restrictions to make things clearer for customers
- Explains what should be included in the RSP's policy statements (if they need one)

2.2. A new row will be added to the Offer Summary for 'service restrictions' to identify things which would not fall within the new traffic management definition but which are important for end users to know. The Offer Summary need only inform the end user that traffic management and/or service restrictions apply on the service and provide a link to a Statement which provides more specific information.

2.3. The Traffic Management and Service Restriction information will be incorporated into the Code when it is next reviewed by the TCF.

3. AUDIENCE

3.1. This document has been written to be read by RSPs so they understand what they need to disclose in their Offer Summary and policy statements.

3.2. The words used in this document have specific technical meanings. For ease of understanding, sample Offer Summary Statements are provided in appendix 1 to show how information should be presented to end users.

4. DEFINITIONS:

Traffic Management means any policy to manage traffic in a way that may affect the relative performance of some or all of an end user's traffic on the plan, or discriminate against another content or network operator on the basis of commercial rivalry.

An example of a Traffic Management policy is giving peer to peer traffic lower priority than other network traffic during network busy periods. Excluded from this definition are:

- Things which are 'opt in' or are configurable by an individual end user
- RSP actions where an end user has violated the RSP's terms and conditions
- Industry best practices to protect customers
- Industry best practices to efficiently manage the network
- Things required by law

Service Restrictions means any policy to prevent access to specific services or activities on the plan. An example of a Service Restriction is voluntarily blocking certain types of websites. Excluded from this definition are:

- Things which are 'opt in' or are configurable by an individual end user
- RSP actions where an end user has violated the RSP's terms and conditions
- Industry best practices to protect customers from, for example fraudulent activity, degraded experience, unwarranted charges or excess data usage.
- Industry best practices to efficiently manage the network
- Things required by law

Industry best practices refers to behaviour which would be deemed by other RSPs to be a proportionate and appropriate response to a likely or actual threat to the network and/or the RSP's end users, or which are fundamental to the functioning of a network, such as prioritizing network control traffic. Industry best practices exclude activities which, on the basis of commercial rivalry, discriminate against another content provider or network operator.

5. OFFER SUMMARY STATEMENT:

If a RSP needs to declare its traffic management or service restrictions policy it should use these words in the Offer Summary.

Traffic Management	We have a traffic management policy in place which may influence your broadband performance. See [insert link] for more details.
Service Restrictions	We have some service restrictions which may impact certain types of customers. See [insert link] for more details.

6. TRAFFIC MANAGEMENT STATEMENT:

6.1. If a RSP has a Traffic Management policy in place it should be disclosed to end users in a Traffic Management statement. A link to this should be provided on its Offer Summary statement for the affected plan, refer to section 5 above. The Traffic Management policy should be publically available and clearly explain the policy in a consumer friendly way.

6.2. Examples of things which **should** be disclosed (unless required by law) include:
- Prioritising (or de-prioritising) of over-the-top services. State whether this is a category of services (eg all streaming video services) or specific named services.

6.3. Examples of things which would be considered reasonable network management and therefore do **not** need to be disclosed:
- Shaping of traffic at an aggregate level to best match the access connection[1].
- Prioritising voice traffic where that service is provided by the RSP, unless it has a significant negative impact on the performance of that network for other uses, i.e. on-net voice traffic (because voice traffic is a legacy service and does not have significant bandwidth requirements).
- Provision of caching and CDNs.
- Interconnect and peering relationships with other ISPs and content providers.
- Blocking denial of service (DoS) attacks.

7. SERVICE RESTRICTIONS STATEMENT:

7.1. If the RSP has Service Restrictions in place it should be disclosed to end users in a Service Restrictions Statement. A link to this should be provided on the Offer Summary statement for the affected plan, refer to section 5 above. The Traffic Management policy should be publically available and clearly explain the policy in a consumer friendly way.

7.2. Examples of things which **should** be disclosed as Service Restrictions (unless required by law) include:
- Blocking sites on the Digital Child Exploitation Filtering System (if this becomes mandatory for all ISPs then this would not need to be declared).
- Blocking of sites believed to be offering or promoting copyrighted material.
- Blocking of sites believed to be offering or promoting adult (eg pornographic) material
- Blocking of sites which offer VPN access.
- Lack of publically accessible IP address as a result of Carrier Grade Network Address Translation (Carrier Grade NAT).
- Redirecting customers' traffic to the RSP's own equipment (such as forcing customers to use the ISPs' own DNS).
- Blocking SMTP traffic (in and outbound) as these services are often used for sending spam.
- Blocking inbound DNS or certain types of email traffic (while this may prevent DoS attacks on DNS infrastructure it also prevents some services being run such as the customer running their own email server).

[1] This is industry best practice for access connections.

APPENDIX: SAMPLE CONSUMER COMMUNICATION

Example Offer Summary statement

If the RSP needs to declare either its traffic management or service restriction policies it should use these words in the Offer Summary.

Traffic Management	We have a traffic management policy in place which may influence your broadband performance. See [insert link (see service restriction statement below)] for more details [link]
Service Restrictions	We have some service restrictions which may impact certain types of customers. See [insert link statement (see below example)] for more details.

Example Traffic Management Policy Statement

- We deprioritise peer-to-peer file sharing traffic during the hours of 4pm and 1am.
- Our ISP TV service is prioritised at all times so you get the best service experience possible.
- [We take our legal obligations seriously and comply with any laws which require us to manage traffic.]

Example Service Restriction Policy Statement

- We block sites on the Digital Child Exploitation Filtering System.
- We block sites which we believe to be offering or promoting copyrighted material or which are offering or promoting adult (eg pornographic) material.
- We use Carrier Grade Network Address Translation (Carrier Grade NAT) technology in our network meaning that your IP address will not be publically accessible.
- We block both inbound and outbound SMTP traffic as these services are often used for sending spam.
- [We take our legal obligations seriously and comply with any laws which require us to restrict services available to our customers.]