

Tesco Mobile Network Management Policy

Network Management Policy

The purpose of Tesco Mobile's Network Management Policy is to be transparent with our customers as to the steps that we may take to ensure that all our customers have access to our Data Service on an equitable basis.

Tesco Mobile continuously monitors network performance to ensure that all its customers have a positive Service experience. Tesco Mobile endeavours to ensure that the Service received by its customers is not impacted through a minority of users placing excessive demand on network resources (e.g., large bandwidths over long periods) or using the Services in a manner that adversely affects the delivery of the Services. Customers shall not use, or permit any third party to use, the Services in a manner that is excessive, unreasonable, abusive, fraudulent, unlawful, automated or artificially generated in a way that circumvents the intended operation of the Services, harmful to the Network, detrimental to other customers, or otherwise inconsistent with the intended use of the Services.

To ensure a good functioning Service is received by all users, Tesco Mobile may implement measures that are application-agnostic to shape traffic so to avoid filling or overfilling a network link or node. Such measures may include a speed quality of service parameters/ limit, and should this measure be relied upon, any such limit would be applied across all applications and users equally and will not impact typical usage which includes streaming and or gaming. Should a customer's data usage become so excessive to risk affecting other network users, Tesco Mobile reserves the right to limit the customer's Service to a level to avoid any adverse effect on others.

In the event that Tesco Mobile becomes aware or is notified that a customer' has or is using the Service in a manner that breaches Tesco Mobile's terms and conditions (including for, hacking, spamming, denial of service or any fraudulent activities) or in a manner which interferes with Tesco Mobile's Service or causes problems for Tesco Mobile and / or impedes other users' experience, then the Service may be suspended by Tesco Mobile. Customers will be notified and given an opportunity to amend their usage and come into compliance with the terms of use of Tesco Mobile Services. For the avoidance of doubt, if the activity is due to a Virus, Malware or a Botnet on the customer's PC, mobile or other terminal device - the account will remain suspended until the customer has demonstrated that the malicious software has been removed and an up-to-date Virus checker has been installed on the device.

Tesco Mobile continuously monitors quality of service (QoS) parameters such as delay, jitter and packet loss in order to maintain a positive Service experience. Such QoS parameters can result in the slowing down of internet access and web pages failing to load. Certain applications such as video or audio applications may suffer from momentary interruptions, and it may take more time to complete a task that involves downloading or uploading data, a file, audio or video from the internet. Tesco Mobile has a capacity management process in place to address and resolve these QoS parameters if they exceed certain thresholds (above which Service may be affected).

Tesco Mobile Network Management Policy

Tesco Mobile will, on an ongoing basis, review, and where required, update its policy to ensure that all of its customers can access data Services.

Glossary of terms:

A Botnet - a collection of compromised computers (including data enabled-handsets) connected to the Internet (these are also known as 'bots'). When a computer becomes compromised, it becomes a part of a botnet." As per above there is no distinction as to whether an individual is using a modem or tethering via a handset.

A Virus/Malware - a computer program that can replicate itself and spread from one computer data enabled handset or terminal device to another, including but not limited to adware and spyware programs that do not have the reproductive ability. A virus is spread from one device to another (in some form of executable code) over a network or the Internet. Malware includes computer worms, Trojan horses, spyware, dishonest adware and other malicious and unwanted software.

Hacking - when an unauthorised person attempts to access another computer, network or system. Infringing on the privacy of others or damage to computer-based property such as files, web pages or software.

Spamming - the distribution of unsolicited commercial advertisements online.

Denial of service - an attempt to make a computer or network resource unavailable to its intended users usually by saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic.

Quality of Service (QoS) metrics measured by Network Management Tools:

Delay - the time it takes for a piece of data (a "packet") to travel across the network from one node or endpoint to another.

Jitter - metric for the variation in delay of packets that flow from one node or endpoint to another through the network

Packet loss - the proportion of packets lost in transit from a node or endpoint to another during a specified time interval.

Network Management Tools:

Tools used by Tesco Mobile to monitor data traffic and to implement measures to manage traffic including in accordance with Tesco Mobile's Network Management Policy.

- Network traffic monitoring systems
- Network security monitoring systems
- Network abuse management process