GO Traffic Management Policy

At GO we aim to provide our customers with the best possible internet experience. To the extent that GO owns or controls those parts of the network that are used to provide internet services, it consistently invests in technology and capacity to ensure that its customers can derive the best possible benefits from internet use.

The internet is a network of networks and capacity is shared across the internet infrastructure, which means that even with the best intentions and with a lot of investment and technical know-how no internet service provider can give end-to-end guarantees about the service. Furthermore, there are internet users who make very heavy use of their service and can sometimes impinge on the use and enjoyment of other users on the same network. There are also occasions where internet traffic increases dramatically, for example in the case of mass email events (spam) and viruses and security threats such as distributed denial of service (DDoS) attacks on internet networks.

With the above in mind, and to provide for all customers to be able to enjoy their internet service and to ensure quality and safety in the network, we may sometimes use traffic prioritisation techniques. At very busy times for internet use on GO's network, specifically where we experience exceptional or temporary network congestion whether actual or expected, different types of internet traffic and applications may be given precedence in accordance with their time-sensitivity.

GO designs its traffic prioritisation policies to cater for the above in a manner that they facilitate those applications that are more sensitive to the time it takes to deliver packets across the internet, most notably voice communication services. Nevertheless, users engaged in activities such as browsing, emailing, streaming audio or video or gaming should normally not be affected by traffic management. In exceptional cases of traffic management, such services may however experience some degradation such as slower loading of websites or buffering of streaming content.

Where users are subscribed to an unlimited usage plan, GO does not limit the bandwidth said users can avail themselves of, nor does it set monthly usage thresholds above which users will be blocked or experience slower internet speeds. At most, very heavy users may have to download data at slower speeds during times where the network experiences particularly heavy traffic, but they will not have restrictions applied to their download capacity. In other words, for GO customers on unlimited internet plans, unlimited really means unlimited.

GO does not monitor and police the types of internet data that you use. It does however abide by legitimate orders it receives from law enforcement authorities empowered by law, such as the Courts of Justice and the Police, to block access to certain illegal content such as for example child abuse and certain pornography.

In order to maintain quality on the network and to protect its users, GO provides a free limited antivirus and spam protection service on some of its internet plans. GO also uses DDoS detection and mitigation technology. In the case of suspected attacks, GO will attempt to screen out malicious traffic. DDoS attacks and action taken against them may sometimes result in temporary slower internet for users.

In spite of the best efforts to maintain quality and security for its users, it is not always possible to guarantee that security attacks do not happen and GO cannot be held responsible for any such occurrences. As a user you should also be aware that you are best placed to guard against such attacks. We highly recommend that you install appropriate software to protect your device and systems from all types of malware.

You should also be aware that when you use certain services, such as peer-to-peer downloading or video or audio streaming from certain sites, you may be unwittingly also installing malicious software on your device. Often such software, known collectively as malware, will gain access to private computer systems, disrupt computing operations on your device, display unsolicited and repetitive advertising and possibly gather sensitive information. It will also most probably slow down your device and hence your internet.