

## D & P Communications Network Management Practices Policy Disclosure

Last Updated November 25, 2019

D & P (D & P) has adopted the following network management practices, performance characteristics, and commercial terms and conditions for its broadband Internet access services in compliance with the Federal Communications Commission's ("FCC's) Restoring Internet Freedom requirements (WC Docket No. 17-108).

These practices, characteristics, terms and conditions are intended to help preserve the Internet as an open framework that enables consumer choice, freedom of expression, end-user control, competition, and freedom to innovate without permission, while permitting D & P to manage its network reasonably. D & P may revise its Network Management Practices Policy from time to time.

### Network Management Practices

D & P utilizes reasonable and responsible network management practices that are consistent with industry standards, and that are tailored to achieve legitimate network management purposes. Because D & P has limited bandwidth, it reasonably manages its network to facilitate Internet usage by all of its customers. D & P Communications uses reasonable and responsible network management practices in an effort to prevent spam, viruses, security attacks, network congestion and other risks that threaten to degrade service.

**Blocking:** D & P does not block or discriminate against lawful content.

**Throttling:** D & P does not throttle, impair or degrade lawful Internet traffic.

**Affiliated Prioritization:** D & P does not prioritize Internet traffic and has no plans to do so.

**Paid Prioritization:** D & P has never engaged in paid prioritization. We don't prioritize Internet for consideration to benefit particular content, applications or devices. D & P does not have plans to enter into paid prioritization deals to create fast lanes.

### Congestion Management

Congestion is an Internet access service problem that can slow web browsing, downloading, and other activities of the customers during certain peak usage periods. Congestion may be caused by capacity limits and bottlenecks in a service provider's own network, or by limitations in the capacity of the Middle Mile transport facilities and services that many rural service providers must purchase from unrelated entities to carry the traffic of their customers between their service areas and the closest Internet nodes. D & P's network management tools will likely change over time to evolve to keep pace with the Internet and related technologies. We will provide updates here and in other appropriate locations if we make significant changes to this Policy.

D & P constantly monitors its network to manage congestion avoiding over utilization of circuits.

If significant congestion problems arise, D & P approach is to determine the source of the problem, and to increase the capacity of the affected portions of its network and/or of its Middle Mile routes where warranted. In the event of congestion, all traffic is classified as neutral until congestion passes.

### **Application-Specific Behavior**

D & P does not favor or inhibit applications or classes of applications. Customers may use any lawful and commercially available application. The D & P network does not discriminate against or target particular types of content. Peer to Peer, streaming video, VoIP, and video downloads are all classified as content neutral. D & P does not manage congestion based on the applications a customer is using. Its network-management scheme is content-neutral. In deciding whether to implement network management practices to alleviate congestion, D & P does not inspect network traffic for content. If congestion occurs, all users (and all users' traffic) would be subject to the network management practices – regardless of content. Further, D & P does not store its end users' traffic information or provide it to third parties, except as required by law.

When D & P implements network management practices to alleviate congestion, most Subscribers will notice no change in their Internet experience. The goal of congestion management is to enable all users to have access to a fair share of the network at peak times, when congestion occasionally occurs. Congestion management largely focuses on the consumption activity of a group of Subscriber accounts that are using a disproportionate amount of bandwidth. As a result, and based on our experience with this technique, we have determined that the large majority of Subscribers will not likely be affected by it. Our experience also shows that when our systems apply the congestion management technique, it is usually only in effect for a very brief period of time. D & P does not unreasonably discriminate against the transmission of lawful network traffic.

D & P anticipates that select parts of the network tend to be in a congested state only for relatively small portions of a day, if at all.

D & P monitors how user traffic is affected by this system and will make adjustments reasonably necessary to ensure that our Internet Subscribers have a high-quality online experience. D & P also routinely evaluates its overall network performance, and periodically endeavors to enhance its network by adding capacity to address congestion and other performance issues as feasible.

There is no hard and fast rule or example available as to how much bandwidth use is too much for a user to trigger D & P's network management technique. The answer really depends on a number of factors, including overall use, time of day, and the number of applications that might be running at the same time.

The point of the technique is to deliver the best overall online experience possible. The technique should help ensure that all Subscribers get their fair share of bandwidth resources to enjoy all that the Internet has to offer – including surfing the Web, reading e-mails, and downloading movies.

As to impact on voice traffic, D & P Subscribers who use VoIP providers that rely on delivering calls over the public Internet may experience a degradation of their call quality when the network is congested. But VoIP calling in and of itself does not use a significant amount of bandwidth. So VoIP

calling in a time of non-congestion will likely not be affected. Yet VoIP service and quality during times of congestion will likely be affected. But D & P absolutely does not discriminate against Subscribers who use VoIP and those who do not, and it does not intentionally degrade VoIP applications or services.

As to streaming video or video downloads, during periods of congestion, any Subscribers who are using a disproportionate amount of bandwidth – no matter the type or content of the online activity, but including for example streaming video or video downloads – may be affected by this technique.

Yet bear in mind that our technique has no ability to determine the applications or protocols being used or the content, source, or destination.

D & P does not block peer-to-peer traffic or applications like BitTorrent or others as part of its current network congestion management technique.

D & P does not normally monitor the content of the traffic or applications of its customers. It undertakes no obligation to monitor or investigate the lawfulness of the applications used by its customers. If any party contacts D & P with a substantial allegation that an application being used by a customer is unlawful, D & P will investigate the matter (including consultation, as it deems appropriate, with attorneys, consultants, federal or state regulators, and/or federal, state or local law enforcement agencies), and will take appropriate actions to deal with the use of applications that are demonstrated to be unlawful.

### **Device Attachment Rules**

Only devices that conform to publicly available industry standards, and that are not harmful to D & P's network, are approved for use. D & P reserves the right to disable devices that cause disruptions to D & P Communication's customers or that are not in compliance with industry standards. In the event that D & P disables a device or denies access to application providers, prompt notice will be given of the decision to deny access to the network or disable a device.

### **Security**

D & P provides customers with unrestricted access to all of the lawful content, services, and applications available on the Internet. D & P uses industry standard tools and utilizes best practices and policies to protect customers from spam, phishing, and other unwanted or harmful online content. When D & P identifies harmful or unwanted online content, it may prevent delivery of such content to customers, or customers may be permitted to identify or inspect content to determine if it is harmful or unwanted. D & P's security methods are not intended to prevent end-users from running any specific applications.

D & P employs commercially appropriate security procedures to protect its network and its customer records from unauthorized access by third parties. D & P does not guarantee that it can protect customers from any and/or all security breaches.

### **Performance Characteristics**

D & P makes every effort to support advertised speeds and will dispatch repair technicians to customer sites to perform speed tests as needed to troubleshoot and resolve speed and application performance caused by D & P's network. D & P measures availability, latency, and aggregate utilization on the network and strives to meet internal service level targets.

However, the bandwidth speed at which a particular distant website or other Internet resources may be downloaded, or the speed at which your customer information may be uploaded to a distant website or Internet location is affected by factors beyond D & P's control, including the speed of the connection from a distant web server to the Internet, congestion on intermediate networks, and/or limitations on your own computer equipment, including a wireless router. In addition, your service performance may be affected by the inside wiring at your premise. Accordingly, you, the customer, must consider the capabilities of your own equipment when choosing a D & P broadband service. Your computers and/or wireless or other networks in your homes or offices may need an upgrade in order to take full advantage of the chosen D & P broadband plan.

For the wireless service, D & P measures Bit Error Rate (BER) and the Received Signal Strength Indicator (RSSI) parameters for transmission rates, latency, and traffic every 15 min. For DSL, Fiber and T1 service, D & P measures traffic every 5 min. All services are best effort.

D & P tests each service for actual and expected access speeds at the time of network installation to demonstrate that the service is capable of supporting the advertised speed. Customers may also test their actual speeds using the speed test located at [www.speedtest.net](http://www.speedtest.net) and may request assistance by calling our business office at 1-800-311-7340.

Based on the network information D & P receives from its monitoring efforts, D & P's network is delivering data transmission rates advertised for the different high-speed Internet services. To be sure, D & P has implemented a program of testing the performance of its network by using a test protocol similar to the one sanctioned by the FCC. We installed specific network performance monitoring equipment at aggregation points across our network and conducted a series of tests using this equipment. D & P reports the results of this testing below. This result applies to both upload and download data rates, and applies for measurements made both at peak times and over a 24-hour period:

Broadband and Wireless internet services are both capable of utilizing real-time internet applications, i.e. VoIP, streaming video, video downloads. Actual speed depends on the customer's service tier.

## Fiber

Advertised (Mb)	Latency (ms)	Tested (Mb)
25	2	24.42/4.98
50	2	48.90/9.93
110	2	107.61/24.80
175	1	171.21/24.75
250	2	246.72/24.79
500	1	490.83/24.80

## HFC

Advertised (Mb)	Latency (ms)	Tested (Mb)
25	8	26.44/5.04
50	8	49.20/5.04
110	8	107.25/4.95
175	8	167.30/10.05
250	8	242.01/10.11

## Commercial Terms

### Service Description

D & P deploys Internet access to its subscribers through hardwired and wireless broadband access technologies via Fiber to the Premise (voice | video | data), Hybrid Fiber Coax (voice | video | data), DSL (voice | data), Wireless (data) and Dialup.

### Pricing

In order to meet the usage and budgetary needs of all of our customers, D & P offers a wide selection of Internet access plan options, including promotional offerings, bundled service choices, and a la carte alternatives.

To find out about D & P pricing on Internet services, visit our website at:

<https://www.d-pcomm.com>, or call 1-800-311-7340 to speak with a customer service representative.

### Usage-Based Fees

D & P Internet service is priced on a flat-fee basis (plus taxes). D & P does not charge end users a usage-based fee for Internet service.

### Impact of Non-BIAS Data Services

The FCC has defined Non-Broadband Internet Access Services (Non-BIAS) to include services offered by broadband providers that share capacity with Broadband Internet Access Services (BIAS) (previously known as "Specialized Services") also offered by the provider over the last-mile facilities.

Real time services, such as Non-BIAS services, include Voice over Internet Protocol (VoIP) and Internet Protocol (IP) video services. D & P offers both VoIP and IP video service to end-users. The VoIP traffic uses private RFC 1918 addresses, dedicated paths for VoIP and QoS on the routers/switches it touches. The QoS priority is based on the source and destination IP. Where VoIP traffic is combined with best effort Internet traffic and QoS priority is employed, the network could endure marginal delays if there are instances of bandwidth contention, although very unlikely.

These non-BIAS data services do not generally adversely affect the last-mile capacity available for the Company's broadband Internet access services, or the performance of such services. Customer should note, however, that significantly heavier use of non-BIAS services (particularly IP video services) or instances of congestion on the network may impact the available capacity for and/or the performance of its broadband Internet access services. The Company will monitor this situation, and appreciates feedback from its customers.

## **Privacy Policy**

D & P reserves the right to monitor usage rates, bandwidth, transmissions and content in order to protect the operation of the network through reasonable network management practices discussed above. D & P affords full access to lawful content, services and applications available on the Internet and does not routinely monitor, inspect or store the network activity and traffic of its Internet service users.

D & P may collect information regarding customer equipment used on the network, including, but not limited to: equipment type, serial number, settings, configuration and software. D & P may also collect performance information to examine the operation of the equipment, services and applications the customer may use on the network, URLs, data transmission rates and latencies, location information, security characteristics, and information about the amount of bandwidth and other network resources the customer is using in connection with uploading, downloading or streaming data to and from the Internet.

Network traffic, activity, performance information, and equipment information monitored or collected by D & P is done so for the sole purpose of reasonable network management purposes.

D & P Network Management Practices Policy is designed to safeguard our network and its users from spam, viruses, phishing, and other unwanted or harmful on-line content, with the intention of providing the best Internet experience possible for our customers. D & P Network Management Practices are not intended, nor implemented, to block consumers from accessing the content and

applications of their choice, deprive consumers of their entitlement to competition, or discriminate against or in favor of certain network traffic.

D & P is required to comply with relevant state and federal laws, regulations and judicial orders. Information may be disclosed to third parties if D & P determines, in its sole discretion that such a disclosure is necessary to protect our interest or the interests of our customer, or is required to comply with legal requirements or orders. This information may also be disclosed in connection with the sale of our business.

D & P does not discriminate against a particular type of online content. D & P provides its Subscribers with full access to all the content, services, and applications that the Internet has to offer. We are committed to protecting Subscribers from spam, phishing, and other unwanted or harmful online content and activities. We use industry standard tools and generally accepted best practices and policies to help it meet this Subscriber commitment. When these tools and policies identify certain online content as harmful and unwanted (such as spam or phishing Web sites), this content is usually prevented from reaching Subscribers. In other cases, these tools and policies may permit Subscribers to identify certain content that is not clearly harmful or unwanted (such as bulk e-mails or Web sites with questionable security ratings), and enable those Subscribers to inspect the content further if they want to do so.

## **Contact Us**

If you have any questions regarding D & P Network Management Practices Policy or would like to file a complaint regarding its network management practices, please contact us at:

D & P Communications  
4200 Teal Road  
Petersburg, MI 49270  
1-800-311-7340  
<https://www.d-pcomm.com/>

If you believe that D & P is in violation of the FCC's Transparency Rules, you may file either an informal or formal complaint with the FCC. <http://esupport.fcc.gov/complaints.htm>.

## **Additional Disclaimers**

The Transparency Rules, as adopted, and D & P Network Management Practices Policy are not intended to affect, alter or otherwise supersede the legal status of cooperative efforts by Internet access service providers and other service providers that are designed to curtail infringement in response to information provided by rights holders in a manner that is timely, effective, and accommodates the legitimate interests of providers, rights holders, and end users.

Furthermore, the Transparency Rules, as adopted, and D & P Network Management Practices Policy do not prohibit D & P from making reasonable efforts to address the transfer of unlawful content or unlawful transfers of content.