ROGERS NETWORK MANAGEMENT POLICY

Wireline

Rogers does not apply technical Internet traffic management practices to our retail wireline Internet service. Instead, we rely on network investments as the primary tool to manage Internet traffic and address potential congestion. We monitor the utilization of the wireline Internet network to maintain the service experience and plan for additional capacity to ensure that our customers continue to receive the broadband speeds they have purchased.

Rogers has mechanisms in place to protect our wireline Internet network from malicious traffic and security threats, such as Denial of Service (DOS) attacks, malware, spam, and fraudulent activity (e.g., modem cloning). We take standard, necessary and reasonable steps to prevent service outages and to ensure that bandwidth usage is optimized efficiently amongst our customers who share the same service node.

Wireless

Rogers relies on network and spectrum investments as the primary tool to manage mobile Internet traffic and address potential congestion. We do have mechanisms in place to protect the Rogers wireless network and our customers from malicious traffic and other security threats, as well as standard network management processes to enable the normal operation of our mobile network.

Specific plans may have Internet traffic management practices applied as outlined in their data management policies (as listed below). However, all traffic is treated equally, including all applications and classes of service.

Rogers Infinite Plans Data Policy