

Acceptable Use and Traffic Management Policy

Policy

This Acceptable Use Policy sets out the rules which apply to use of our communication services, including your responsibilities and permitted and prohibited uses of those services. Compliance with this Policy ensures you may continue to enjoy and allow others to enjoy optimum use of our Services.

Responsibilities

You are responsible for your actions on our network and systems you access through your Service. If you act recklessly or irresponsibly in using your Service, or your actions endanger any person or the integrity or security of our Network, systems or equipment, your access may be restricted, suspended or terminated, without prior notice.

In particular, you agree that you will not use, attempt to use or allow your Internet Service to be used to:

- store, send or distribute any content or material which is restricted, prohibited or otherwise unlawful under any applicable law or which is likely to be offensive or obscene to a reasonable person;
- store, send or distribute confidential information, copyright material or other content, which is subject to third party intellectual property rights, unless you have a lawful right to do so;
- store, send or distribute material which defames, harasses, threatens, abuses, menaces, offends, violates the privacy of, or incites violence or hatred against, any person or class of persons, or which could give rise to civil or criminal proceedings;
- do any other act or thing which is illegal, fraudulent or otherwise prohibited under any applicable law or which is in breach of any code, standard or content requirement of any other competent authority;
- store, send or distribute material, which interferes with other users or restricts or hinders any person from accessing, using or enjoying the use of our Services, Network or systems;
- forge header information, email source address or other user information;
- access, monitor or use any data, systems or networks, including another person's private information, without authority or attempt to probe, scan or test the vulnerability of any data, system or network;
- compromise the security or integrity of any network or system including our Network;
- deliberately access, download, store, send or distribute any viruses or other harmful programs or material;

- send or distribute unsolicited advertising, bulk electronic messages or otherwise breach your spam obligations set out in this policy, or overload any network or system including our Network and systems;
- use another person's name, username or password or otherwise attempt to gain access to the account of any other User without their consent;
- tamper with, hinder the operation of or make unauthorised modifications to any network or system; or
- aid, abet, encourage or incite any other person to do or attempt to do any of the above acts

Spam

Also known as junk mail or Unsolicited Commercial Email (UCE), the term "spam" refers to submitting a commercial email or SMS messages to a large number of recipients who have not requested or opted to receive it and have no reasonable expectation to receiving email or SMS from the sender.

Email or SMS sent by a company or an organisation with whom the recipient has established a relationship, or which was requested or accepted (opt-in requirement) by the recipient is not considered spam. Spamming is not only harmful because of its negative impact on consumer attitudes toward CDGL, but also because it can overload CDGL's network and disrupt service to CDGL subscribers.

As a user of a CDGL service platforms you must comply with any regulation in force that covers direct marketing regulations, if you are sending communications to large multiple lists of users.

In the absence of positive, verifiable proof to the contrary by a User, CDGL will consider complaints by recipients of emails or SMS messages to be conclusive that the recipient did not subscribe or otherwise request the email(s) or SMS about which a complaint was generated.

Excessive Use

You must use your Service in accordance with any download or capacity limits stated in the specific plan that you subscribe to for the use of that Service. We may limit, suspend or terminate your Internet Service if you unreasonably exceed such limits or excessively use the capacity or resources of our Network in a manner which may hinder or prevent us from providing services to other customers or which may pose a threat to the integrity of our Network or systems.

If CDGL determines that excessive call volumes, bandwidth, disk space utilisation or high CPU loads are adversely affecting CDGL's ability to provide service to other users or impacting CDGL's commercial model, CDGL may take immediate action, which may include suspension or termination, without notice, of the service.

Reasonable Use

Where a data service is specified as unmetered or unlimited use, reasonable usage is considered to be within 500 GB per month. Where this usage is exceeded, CDGL reserves the right to apply policies in traffic management to limit or restrict the usage above this level or to terminate the

User's access to the Services if the limits continue to be exceeded after notification to the User.

Where a call package includes 'unlimited calls', the customer must not use diallers or any system/apparatus that would unnaturally inflate the level of outbound traffic beyond that considered by CDGL to be normal usage.

Illegal Use

The CDGL network may only be used for lawful purposes. For example, Users may not use the CDGL Network to create, transmit, distribute, or store content that:

- violates a trademark, copyright, trade secret or other intellectual property rights of others,
- violates export control laws or regulations,
- violates the privacy, publicity or other personal rights of others,
- impairs the privacy of communications,
- contains obscene, offensive, unlawful, defamatory, harassing, abusive, fraudulent, or otherwise objectionable content as reasonably determined by CDGL,
- encourages conduct that would constitute a criminal offense or give rise to civil liability,
- constitutes deceptive online marketing,
- causes technical disturbances to the CDGL network, its affiliated networks, or the network used by Users to access the Email service, or
- violate the policies of such networks, including, but not limited to, intentional introduction of any viruses, Trojan horses, worms, time bombs, cancel bots or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system or data, or
- assists, encourages or permits any persons in engaging in any of the activities described in this section. If the Client becomes aware of any such activities, the Client is obligated to immediately notify CDGL and take all other appropriate actions to cause such activities to cease.

Consequences of Unacceptable Use

CDGL reserves the right to suspend or terminate User's access to the Services upon notice to the Client of a violation of this policy, or without notice, where in CDGL's opinion this is necessary. If CDGL believe that the policy has been breached or the integrity of the network and/or the performance of other users are at risk, then CDGL will contact the Client with notice of its intent or to notify the User of the breach of the policy.

Broadband Traffic Management Policy

We undertake traffic management to ensure that our Clients and Users receive optimum performance at all times. The policy applied is as follows:

Traffic Management

Our broadband products are subject to traffic management to ensure you receive optimum performance at all times.

Like other providers we deliver broadband service over a shared network. To provide a sustainable quality broadband service to all our customers we may apply traffic management policies to network.

The principles of our network management policies are:

- To make sure that time-critical applications like Voice over Internet Protocol (VoIP) are always prioritised.
- To protect interactive applications like web-browsing and Virtual Private Network (VPN) from non-time sensitive download traffic.
- To balance the network under demand to cope with exceptional peaks and troughs from day to day and month to month.
- Provides a 'quality of service' effect, meaning multiple applications running on the same line interact with each other effectively, and use of high demand protocols like Peer-to-Peer (P2P) doesn't swamp time-sensitive traffic such as a VoIP call.

Traffic types are identified in real-time based on a combination of port, source IP address and DPI signature detection. This allows us at any given time to see exactly what traffic is on the network and who is doing what.

At times we may prioritise time sensitive traffic such as VoIP by reducing the throughput of the standard traffic.

Mobile

You must not use our SIM cards to generate artificially inflated traffic or to persistently send automated or unsolicited text messages.

Avoid sending unusually high volumes of SMS messages, sending SMS messages to an unusually

large number of recipients or distribution groups or sending any automated or unsolicited SMS messages. Furthermore, sending spam text messages would breach this Acceptable Use Policy. You must not establish, install or use a gateway device or SIM box without our prior written consent (including devices tethered via cable, Bluetooth or Wi-Fi, to a computer or the internet, when used for making large volumes of calls or sending large volumes of texts). We can withhold our consent for this activity at our absolute discretion.

You must not use a SIM Card fraudulently, in connection with a criminal offence, in breach of

any law or statutory duty, to make a call or send a message or to take pictures or video or send, upload, download, use or re-use any material, which is offensive, abusive, indecent, defamatory, obscene or menacing, a nuisance (including to our staff) or a hoax in breach of any rights or anyone's privacy, or is otherwise unlawful.

Avoid making nuisance phone calls, unlawful file sharing, and sharing, downloading or viewing inappropriate or illegal content are examples of use that would fall outside this Acceptable Use Policy.

You may only use our Roam Like at Home service in our Europe Zone (excluding the UK) for periodic travel, like holidays or short breaks. If you're not genuinely using our services for periodic travel, we may have to charge you for, or suspend you from, using our services in our Europe Zone (excluding the UK).

Avoid using our services for the first time outside of the UK, using a large volume of your allowance in our Europe Zone (excluding the UK), or for prolonged periods which don't follow reasonable consumer holiday and travel patterns and behaviour. If you use our services outside the UK in our Europe Zone for 60 or more days in any four-month period, this is likely to be deemed to be an unfair use of our services. You will be notified if you are in breach of our Acceptable Use Policy and you will have two weeks from that moment to rectify your behaviour before you receive out-of-bundle charges at the prevailing rate.

Remember, the points above are not an exhaustive list of how you could be breaching our Acceptable Use Policy for our various products and services. Other activities which we reasonably believe to be outside of legitimate use may also be subject to the terms in this Acceptable Use Policy.

Administration of Policy

The Client understands that the administration of this policy requires the exercise of discretion and judgment by CDGL. CDGL agrees to exercise good faith in its administration of this policy and in making determinations under the policy.