PTLGateway Acceptable Use Policy

Last Updated Date: 02 March 2018

Acceptable Use Policy

Your use of our Services must fall within our Acceptable Usage Policy.

Contents

Key details

This Acceptable Use Policy (A.U.P.) may be subject to change from time to time and without prior notice.

COVERAGE OF THIS POLICY AND AGREEMENT

In addition to other agreements between you and PTLGateway, this policy and agreement does two things:

1. it explains the acceptable use policy (the “Acceptable Use Policy”) that governs our Services, including the actions that we may, within our sole discretion, take for any use that we deem unacceptable; and
2. it enumerates the terms and conditions under which you agree to use our Services.

By accessing or using our Services, you consent to the acceptable use practices described in this Policy and to the terms of this Agreement (collectively the "Acceptable Use Policy"), as modified from time to time by PTLGateway. "You" includes anyone who uses our Services. The purpose of this Policy and Agreement is to protect our Network, our customers, and others from inappropriate, unauthorized, illegal or otherwise objectionable activities. Please read this Policy and Agreement together with our Privacy Policy, Master Services Agreement and any other applicable policies. If you do not agree to accept and comply with the terms of this Policy and Agreement, including all documents, policies and guidelines incorporated herein, please don't use our Services.

YOUR RESPONSIBILITIES

You are responsible for any transmission you send or receive through our Network, including the content of any communication. PTLGateway does not actively monitor, censor, or directly control any information that is stored on or transmitted over our Network or third party sites or services that are accessible by through our Services.

Consequently, we do not warrant, verify or guarantee the quality, accuracy, or integrity of the information that you may access. Nor do we accept any responsibility whatsoever for such information. Although we strive to provide useful and accurate information, errors may appear from time to time.

Before you act on information you've found on our Network, you should confirm any facts that are important to your decision. Your access to any such information is at your risk. We are not responsible for, and cannot guarantee the performance of, goods and services offered through our Services. You must also exercise best efforts to ensure the security and integrity of your own network; to detect and prevent unauthorized access to your network or PTLGateways network; and to take commercially reasonable steps to safeguard passwords, personal identification numbers, or other access or authentication devices.

We provide a number of tools and solutions to assist customers in monitoring their use of our Services and the data that they store. Training and guidance on the use of these tools is available.

It is the responsibility of the Customer to ensure they comply with the latest version of the A.U.P. Use of the Service for the first time is deemed to indicate the Customer's acceptance of the Terms and Conditions and Acceptable Use Policy. This A.U.P. is a guideline for responsible use of the Service and is not intended to be exhaustive. In order for the complex arrangement of systems commonly known as the "PTLGateway" to function correctly, those who connect to it must do so in accordance with generally accepted standards and conventions. PTLGateway may take any appropriate steps against any Customer who is responsible for abuse of the Service.

This may include, but is not limited to, a formal warning, suspension of the Service or suspension of all Services supplied by the Company, without prejudice to any accrued rights of the parties. The Customer agrees to use the Services in a lawful manner at all times and to observe the provisions of the Data Protection Act 1998. The Customer will indemnify the PTLGateway against any damages, costs or loss suffered directly or indirectly as a result of any breaches of this A.U.P. by the Customer.

Without limitation, the Customer's attention is drawn to the following:

You may not violate the security of our Network in any way. Such violations may result in criminal or civil liability. PTLGateway may, but is not obligated to, investigate any violation. PTLGateway may cooperate with law enforcement where criminal activity is suspected.

By using the Services, you agree to cooperate, as well, in any such investigation. Examples of Network security violations include, without limitation.

- Hacking: Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network.
- Interception: Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network. ·Intentional Interference: Interference with service to any user, host or network including, without limitation, denial-of-service attacks, mail bombing, news bombing, other flooding techniques, deliberate attempts to overload a system and broadcast attacks.
- Falsification of Origin: Forging of any TCP-IP packet header, e-mail header or any part of a message header. This prohibition does not include the use of aliases or anonymous remailers.
- Avoiding System Restrictions: Using manual or electronic means to avoid any use limitations placed on the Services, such as timing out.

The Company will not tolerate any thoughtless or malicious activity that may damage or impair the proper functioning of any PTLGateway equipment or Service the use of any Service by any other customer.

The Customer must not use the Service for any illegal activity. Be aware that any access to any computer system without explicit authorisation may be a criminal offence under the Computer Misuse Act 1990.

Traffic over the Global Internet may traverse other networks or services not owned or operated by PTLGateway. The Customer must comply with the A.U.P. and other terms and conditions imposed by the operators of those networks and services. PTLGateway may, but is not obligated to, take any action it deems necessary to protect its Network, its rights or the rights of its customers or third-parties, or optimize or improve its Network, services, systems, and equipment. You acknowledge that such action may include, without limitation, employing methods, technologies, or procedures to filter or block messages sent through the Network. PTLGateway may, in its sole discretion, at any time, filter “spam” or prevent “hacking,” “viruses” or other potential harms without regard to any preference.

E-mail Services

There are many forms of e-mail abuse, this document is a guideline for responsible use of the Service and is not intended to be exhaustive. Use of e-mail is generally a matter of common sense and courtesy to others. This Acceptable Use Policy (A.U.P.) may be subject to change from time to time and without prior notice.It is the responsibility of the Customer to ensure they comply with the latest version of the A.U.P. Use of the Service for the first time is deemed to indicate the Customer’s acceptance of the Terms and Conditions and Acceptable Use Policy.

Illegal Content

Acts of Parliament make it illegal to transmit certain material on a public telecommunications network. It is not acceptable to send such material by e-mail. Similarly, the sending of copyrighted material or intellectual property without the owner's permission is not permitted. PTLGateway does not permit abuse of the Service in any way, including those listed below and will take any appropriate steps against any Customer who is responsible for such abuse. This may include, but is not limited to, a formal warning, suspension of the Service or suspension of all Services supplied by the Company, without prejudice to any accrued rights of the parties. The Customer agrees to use the Services in a lawful manner at all times and to observe the provisions of the Data Protection Act 1998. The Customer will indemnify PTLGateway against any damages, costs or loss suffered directly or indirectly as a result of breaches of this A.U.P. by the Customer.

Denial of Service

Denial of Service attacks may be a criminal offence under the Computer Misuse Act 1990. A Denial of Service attack is any activity with the aim or effect of interfering with the normal operation of some electronic system. This includes, but is not limited to:

- E-mail bombing in such a way as to make the normal use of some service impossible, difficult or costly
- Intentionally sending e-mail intended to damage the receiver's systems. For example, sending malicious or "virus" programs attached to an e-mail message
- Opening an excessive number of connections to one system
- Using e-mail relaying or similar services without authorisation to do so ·Chain Letters, "Make Money Fast" and Pyramid-Selling Schemes: These messages are similar to their paper versions. They rarely offer any material or financial reward and waste resources for Internet service providers and those who download them. The Customer agrees not to originate or take part in the propagation of any such message.

Unsolicited Commercial E-mail

Unsolicited Commercial E-mail is advertising material sent and received by e-mail without the recipient requesting such information. It may be unlawful under the Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulations 1998.

Please note that by visiting a web side, taking part in an online discussion or similar a user has not expressed their interest in receiving such e-mail, unless they have made an explicit request for information to be sent to them. We draw you attentions the regulations covering this with GDPR.

Unsolicited Bulk E-mail

This is similar to Unsolicited Commercial E-mail, but not necessarily advertising any product or service. Its usual sole purpose is to annoy.

E-mail Bombing

E-mail bombing is the sending of many or a single large message with the sole intent of annoying some other Internet user or group of users.

The sending of very large e-mail messages without prior agreement can constitute a denial of service at the receiving site.

E-mail List Subscriptions

E-mail lists are schemes for distributing copies of messages to many different people. It is not acceptable to subscribe any other person to an e-mail list without having their explicit permission to do so.

Forgery

Forgery means sending e-mail such that its origin or transmission path appears to be something other than that which it really is. It is also forgery to arrange for replies to be sent to some other user or system. However, such activities can have genuine uses and are acceptable provided the relevant parties have granted their permission.

Data Breaches

PTLGateway Information Security is committed to protecting PTLGateway's employees, partners, customers and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

If a customer suspects or is aware of a data breach this should be registered with PTLGateway, (see PTLG Data Breach Response Policy) and we will investigate and assist.

As the Data Controller it is the Customers responsibility to report Data breaches to the Information commissioner.

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

https://ico.org.uk/for-organisations/report-a-breach/

The Customer is responsible for the accuracy and integrity of any personally identifiable information they collect, store or transmit via our systems. You must take measures to ensure the data you hold is consistent with both the legal and spirt of General Data Protection Regulations,

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

If PTLGateway detects or suspects a data breach has occurred that might impact your data then we will inform you as soon practical and agree the action plan to be followed. Refer to PTLGateway's Security Breach Policy document.

Modification of the Policy and Agreement

We reserve the right to modify this Policy and Agreement at any time, effective upon its posting, as modified, on www.ptlgateway.net. By using the Services, you agree to abide by this Policy and Agreement, as modified from time to time. You should refer to this Policy and Agreement to ensure that your activities comply with the most recent version.

If you have any questions about this policy, please contact us

https://helpdesk.ptlgateway.net/conversation/new