ACCEPTABLE USE POLICY (AUP)
RIDGEON NETWORK LTD

Last Revision: 05 March 2025
Author: Chris Ridgeon

Reference: RN_AUP
Classification: PUBLIC

Document History

Reference/Version	Date	Author	Reason/Changes
RN_AUP_180522	22 May 2018	C.Ridgeon	Updated tracked version in Quality Management System to replace last Revision 06 Jan 2014 and updated content.
RN_AUP_180530	30 May 2018	C. Ridgeon	Updated reference of Data Protection Act
RN_AUP_220609	09 June 2022	C.Ridgeon	Reviewed as part of continued ISO audits. No changes required.
RN_AUP_250305	05 March 2025	C.Ridgeon	Reviewed as part of continued ISO audits. No changes required.

01455 221 645 info@ridgeon-network.co.uk www.ridgeon-network.co.uk
Ridgeon Network Ltd, Alma Park, Woodway Lane, Claybrooke Parva, Lutterworth, Leicestershire, LE17 5BH

ACCEPTABLE USE POLICY (AUP)
RIDGEON NETWORK LTD

This Acceptable Use Policy (AUP) is intended to help protect Ridgeon Network customers, and the Internet community, from the inappropriate use of the Internet. A customer's use of Ridgeon Network service constitutes acceptance of this AUP and Ridgeon Network's Terms and Conditions document. Ridgeon Network reserves the right to revise and update this AUP from time to time. Ridgeon Network expects customers to cooperate with the company's Abuse department when requested to assist in their investigations.

THIS AUP IS DIVIDED INTO TWO PARTS:

Part 1.
Violations and Descriptions of Appropriate Use
Part 2.
Reporting to Ridgeon Network's TOS/Abuse department

PART 1: VIOLATIONS AND DESCRIPTIONS OF ACCEPTABLE USE
1.1 GENERAL VIOLATIONS

Our AUP prohibits the following:

Impersonation/Forgery - Adding, removing, or modifying identifying network header information ("spoofing") in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited. The use of anonymous re-mailers and nicknames does not constitute impersonation. Using deliberately misleading headers ("munging" headers) in news postings in order to avoid spam e-mail address collectors is allowed provided appropriate contact information is contained in the body of the posting.

Privacy Violations - Attempts, whether successful or unsuccessful, to gain access to any electronic systems, networks or data, without proper consent, are prohibited.

Threats - Threats of bodily harm or destruction of property are prohibited.

Harassment - Threatening or harassing activity is prohibited.

Illegal Use - The use of any Ridgeon Network service for illegal purposes is prohibited.

Reselling - The resale of any Ridgeon Network service without proper authorisation from Ridgeon Network Ltd. is prohibited. Persons wishing to act as resellers may review details of the Ridgeon Network Partner Programme, available upon request.

Copyright Infringement - All material published must be owned by the publisher or the appropriate releases must have been obtained prior to publishing. Ridgeon Network will co-operate with all agencies attempting to assert their rights in these matters.

1.2 NETWORK DISRUPTIONS AND NETWORK-UNFRIENDLY ACTIVITY

Any activities, which adversely affect the ability of other people or systems to use Ridgeon Network services or the Internet, are prohibited. This includes "denial of service" (DoS) attacks against another network host or individual user. Interference with, or disruption of, use of the network by others, network services or network equipment is prohibited.

It is the customer's responsibility to ensure that their service is configured in a secure manner. A customer may not, through action or inaction, allow others to use their service for illegal or inappropriate actions. A customer may not permit their service, through action or inaction, to be configured in such a way that it gives a third party the capability to use their service in an illegal or inappropriate manner.

1.3 E-MAIL

Ridgeon Network does not tolerate, endorse or participate in e-mail spamming. Sending unsolicited commercial e-mail is prohibited. We cannot authorise bulk e-mailing although we do recognise that in some instances this is a valid and useful form of marketing for both senders and recipients.

Using a Ridgeon Network e-mail or Web site address to collect responses from unsolicited commercial e-mail is prohibited.

Sending large volumes of unsolicited e-mail, whether or not that e-mail is commercial in nature is prohibited.

Activities that have the effect of facilitating unsolicited commercial e-mail, or large volumes of unsolicited e-mail, whether or not that e-mail is commercial in nature, are prohibited. Users operating mail servers must ensure that they are not open relays.

Anonymous bulk e-mailings are not permitted and we will terminate the accounts of any customers who attempt to do this. This may happen without notice.

If we receive any complaints from recipients or other third parties, or any mailing causes technical problems on our systems, we may take further action to stop this happening again. This may involve the termination of any

accounts the sender has and may occur without notice. In the event that we are alerted to anyone sending bulk e-mails, we will generally attempt to make contact with the senders to discuss appropriate actions.
We recommend that anybody undertaking this kind of activity has a data protection statement on their Web site explaining how the company fulfils their obligations in terms of the applicable data protection laws.
Senders must give recipients the ability to easily contact the sender and remove themselves from their mailing list.
Senders must be sure that recipients are aware that they are listed on the sender's e-mailing list and that they themselves provided their information or authorised a third party to do so on their behalf.
Senders must make every effort to ensure that the information they are sending is of interest to the recipient and matches the reason given for the collection of the e-mail address in the first place.
In the event of any problems being caused by this type of activity, we will make every effort to ensure that the problem is resolved as quickly as possible. This includes full co-operation with any relevant authorities.

1.4 FACILITATING A VIOLATION OF THIS AUP

Advertising, transmitting, or otherwise making available any software, programme, product, or service that is designed to violate this AUP, or the AUP of any other Internet Service Provider, which includes, but is not limited to, the facilitation of the means to spam.

1.5 NEWS

Ridgeon Network customers should use their best judgment when posting to any newsgroup. Many groups have charters, published guidelines, FAQs, or ‘community standards’ describing what is and is not considered appropriate. Usenet can be a valuable resource if used properly. The continued posting of off-topic articles is prohibited. Commercial advertisements are off-topic in most newsgroups, especially non-commercial regional groups. The presence of such articles in a group is not indicative of the group's intended use. Please familiarise yourself with basic USENET netiquette before posting to a newsgroup.
Newsgroup spamming: Spam is, first and foremost, a numerical metric-posting of substantively similar articles to multiple newsgroups. This form of spam is sometimes referred to as "excessive multi-posting" (EMP). Ridgeon Network considers ‘multi-posting’ to 10 or more groups within a two-week period to be excessive.
Hostile attacks or invectives (flames) aimed at a group or an individual poster are generally considered inappropriate in Ridgeon Network service groups. Flames in the non-service groups are discouraged. Many newsreaders offer filtering capabilities that will bring certain messages to your attention or skip over them altogether (kill files).
Ridgeon Network customers may not cancel messages other than their own messages. A customer may cancel posts forged in that customer's name. Ridgeon Network may cancel any postings that violate this AUP.

1.6 WEB

Using a Ridgeon Network Web site address or Ridgeon Network hosted Web account for the purpose of distributing illegal material is prohibited. Ridgeon Network will co-operate with authorities to remedy breaches of this policy.

Using a Ridgeon Network Web site address or Ridgeon Network hosted Web account to collect responses from unsolicited commercial e-mail is also prohibited.

1.7 EXCESSIVE BANDWIDTH OR RESOURCE UTILISATION

Ridgeon Network service descriptions specify current limits on bandwidth and disk utilisation. Where limits are not specifically defined or are defined as ‘unlimited’ the judgement of the Ridgeon Network Technical Support team shall be used to define those limits. The use of bandwidth or disk space in excess of those limits is not permitted.
The total number of bytes transferred from an account’s Web and FTP space determines bandwidth utilisation.
The total number of bytes required to store an account’s Web, FTP, and Mail data determines disk utilisation.
If Ridgeon Network determines that excessive bandwidth or disk space or other resource utilisation is adversely affecting Ridgeon Network's ability to provide service to you and/or other customers, Ridgeon Network may take immediate action. Ridgeon Network will attempt to notify the account owner by e-mail as soon as possible.

2. REPORTING TO RIDGEON NETWORK'S ABUSE DEPARTMENT

Ridgeon Network requests that anyone who believes that there is a violation of this AUP should direct the information to the AUP Abuse Staff at abuse@ridgeonnet.com. Ridgeon Network customers who wish to report 'spam' from a non-Ridgeon Network source should send copies of the e-mail they received along with full header information. Some messages may not receive a response, but Ridgeon Network may use the information received at this address to aid in the development of Ridgeon Network's filter lists.
All issues involving other e-mail abuse originating from Ridgeon Network e-mail or network addresses should also be sent to the above address, along with all issues regarding USENET 'news' abuse issues originating from Ridgeon Network customers, other suspicious activity such as port scans or attempts to penetrate network resources and virus distribution and copyright infringement.

RIDGEON NETWORK MAY TAKE ANY ONE OR MORE OF THE FOLLOWING ACTIONS IN RESPONSE TO COMPLAINTS:

- Issue warnings: written or verbal
- Suspend the customer's newsgroup posting privileges
- Suspend the customer's account and/or services without reimbursement
- Terminate the customer's account and/or services without reimbursement
- Invoice the customer for administrative costs, loss of service and/or reactivation charges
- Amend the service configuration/setup to prevent the issue or reduce impact

TO REPORT ABUSE, WHAT INFORMATION SHOULD BE SUBMITTED?

- The IP address used to commit the alleged violation
- The date and time of the alleged violation, including the time zone or offset from GMT
- Evidence of the alleged violation

Copies of e-mail with full header information provide all the required information, as do syslog files and firewall logs. Other situations will require different methods.