

Redalto Communications Acceptable Use Policy

Redalto Communications' (Redalto) "Acceptable Use Policy" (AUP) is intended to promote safe and secure use of Internet Services for its customers. Additionally the AUP is intended to maintain integrity of Redalto's infrastructure by prohibiting unacceptable use of IP services. All users of Redalto's services should make every effort to comply with this Policy.

Considerations

In general the Internet is as secure as any other common communications medium including post, facsimile and voice telephone service. However the Internet is an open infrastructure connecting networks, companies, and individuals from all around the world. Redalto Communications therefore advises that its customers be prudent and take appropriate measures to protect themselves and secure their Internet communications.

Redalto will comply with all applicable laws concerning the privacy of its Customers' on-line communications and use all reasonable efforts to maintain and improve the security of its services. However, Redalto takes no responsibility for the security of content transmitted over the Internet by its customers, including any part of Redalto's network that could be considered to form part of the Internet.

Acceptable Uses of Redalto's Network and Services

A User may use Redalto's network and Services for any activity allowed by law, subject to the terms and conditions of User's Service Agreement with Redalto. Redalto also recommends that each of its Users take the following measures to ensure that neither the User nor any of its end users violate this AUP:

- a. Educate your end users about standards, including without limitation this AUP, governing their use of the User's network, Redalto's network and the Internet in general
- b. Use a Firewall and enforce limitations on authorized connections into the organization's network for all incoming and outgoing network traffic.
- c. Scan all mail for malicious content.
- d. Ensure all accounts have a password and that the passwords are difficult to guess.
- e. Be vigilant in network use and configuration, making changes as vulnerabilities become known.
- f. Keep your systems up-to-date with upgrades and patches. Regularly check with vendors for the latest available patches, fixes and upgrades.
- g. Regularly check on-line security archives such as those maintained by incident response teams for security alerts and technical advice.
- h. Audit systems and networks, and regularly check logs. Configure systems so that adequate logs are generated
- i. When using a mailing list, confirm that all of the recipients on the list have requested or otherwise affirmatively accepted receipt of materials being sent to the list;
- j. Promptly investigate and, if necessary, respond to security breaches or violations of use policies by your end users; and
- k. Ensure that Redalto has up-to-date contact information of User's organization so that Redalto can promptly notify User of changes to the AUP, possible violations, and related notifications.

Unacceptable Uses of Redalto's Network and Services

Each of the following uses of Redalto's network and/or Services is considered to be harmful to its customers, affiliates, and/or its network, operations, Services or reputation. It therefore is a violation of the AUP and shall entitle Redalto to exercise any and all remedies available to it under its Service Agreement with the User, this AUP and applicable laws:

- a. Illegal Use - Using the Services to transmit any material (by email, uploading, posting, or otherwise) that violates any applicable local, national or international law or regulation.
- b. Threats - Using the Services to transmit any material (by email, uploading, posting, or otherwise) that threatens or encourages bodily harm or destruction of property.
- c. Harassment - Using the Services to transmit any material (by email, uploading, posting, or otherwise) that harasses another person or entity.
- d. Offensive or Discriminating Content - Using the Services to disseminate offensive or discriminatory content, including racist, sexist, homophobic, disablist, sexually explicit or abusive material.
- e. Fraudulent Activity - Using the Services to make fraudulent offers to sell or buy products, items, or services or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters."
- f. Forgery or Impersonation - Adding, removing or modifying identifying network header information in an effort to deceive or mislead. Attempting to impersonate any person by using forged headers or other identifying information. The use of anonymous re-mailers or nicknames does not constitute impersonation. Using deliberately misleading headers ("munging" headers) in news postings in order to avoid spam email address collectors is allowed.
- g. Unsolicited Commercial Email / Unsolicited Bulk Email - Using the Services to transmit any unsolicited commercial email or unsolicited bulk email. Activities that have the effect of facilitating unsolicited commercial email or unsolicited bulk email whether or not that email is commercial in nature are prohibited.
- h. Unauthorized access - Using the Services to access, or to attempt to access, the accounts of others, or to penetrate, or attempt to penetrate, security measures of Redalto's or another entity's computer software or

hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in the corruption or loss of data. Also use of the Services in a manner or to an extent not agreed upon by User and Redalto in the fully executed Services contract for such Services.

- i. Copyright or Trademark Infringement - Using the Services to transmit any material (by email, uploading, posting, or otherwise) that infringes any copyright, trademark, patent, trade secret, or other proprietary rights of Redalto or any third party, including, but not limited to, the unauthorized copying of copyrighted material, the digitisation and distribution of photographs from magazines, books or other copyrighted sources, and the unauthorised transmittal of copyrighted software.
- j. Collection of Personal Data -Using the Services to collect, or attempt to collect, personal information about third parties without their knowledge or consent.
- k. Reselling the Services - Reselling the Services without Redalto's written approval.
- l. Network Disruptions and Unfriendly Activity -Using the Services for any activity that adversely affects the ability of other people or systems to use Redalto Services or the Internet. This includes "denial of service" (DoS) attacks against another network host or individual user. Interference with or disruption of other network users, network services or network equipment is prohibited. It is the User's responsibility to ensure that their network is configured in a secure manner. A User may not, through action or inaction, allow others to use their network for illegal or inappropriate actions. A User may not permit their network, through action or inaction, to be configured in such a way that enables a third party the capability to use their network in an illegal or inappropriate manner.

Detection of Violations.

Redalto does not review, edit, censor or take responsibility for the content of information and communications that its Users transmit, receive, distribute or store via Redalto's network and Services. However, Redalto reserves the right to monitor information and/or communications transmitted over its network when;

- a. in Redalto's reasonable judgment, such monitoring is necessary to protect its Customers or its network from damage or liability;
- b. Redalto has a reasonable belief, supported by verifiable information, that this AUP or any applicable law has been or is being violated;
- c. required to do so by law, or by the order of a court or government agency; or
- d. monitoring is necessary to ensure that Redalto's network is operating within acceptable parameters with regard to certain service levels and technical specifications.

Redalto will not disclose any information or communications sent or received by its Users unless required to do so by law or to the extent necessary to comply with the order of a court or government agency. Redalto's disclosure of User information is also governed by any confidentiality provisions (if any) of its Services contract with the User. Redalto also complies with all laws related to the disclosure of its Users personal data.

Users of Redalto Services will cooperate with Redalto in any corrective action that Redalto deems necessary in order to prevent the transmission, distribution or storage of information or communications that are in violation of this AUP. A User's failure to co-operate with such corrective measures is a violation of this AUP, and Redalto may suspend its provision of Services, wholly or in part, to such User upon 24 hours prior notice (or, in emergencies, without prior notice) as a result of such failure.

Reporting Violations

If you believe that a violation of this AUP has occurred, please contact Redalto at [abuse \[a\] redalto.com](mailto:abuse@redalto.com).

If available, please provide the following information:

- The email, IP address, or other identifying information of the entity who committed the alleged violation
- The date and time of the alleged violation, including the time zone or offset from GMT
- Evidence of the alleged violation

Responsibility of Customers for Activities of Their End Users

Any actual or attempted violation of this AUP by any person who the User allows to use the Services shall be a violation of the AUP by the User.