
The People. The Technology. The Solution.
entitydata®
Acceptable Use Policy (AUP)

One important aspect of the Internet is that no one party owns or controls it. This fact accounts for much of the Internet's openness and value, but it also places a high premium on the judgment and responsibility of those who use the Internet, both in the information they acquire and in the information they disseminate to others.

This AUP forms part of the terms of your Agreement with Entity Data. Capitalised terms used but not defined in this AUP shall have the meanings given to them in the Terms and Conditions. Your Services may be suspended or terminated for breach of this AUP in accordance with the Entity Data Terms of Conditions of Service. You are responsible for violations of this policy by you or anyone using the Services, whether authorised by you or not. If you have any questions, please contact us abuse@entitydata.com.au

1. Internet Abuse

You may not use our network to engage in illegal, abusive, or irresponsible behaviour, including:

1.1 unauthorised access to or use of data, services, 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 authorisation of the owner of the system or network;

1.2 monitoring data or traffic on any network or system without the authorisation of the owner of the system or network;

1.3 interference with Service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;

1.4 use of an Internet account or computer without the owner's authorisation;

1.5 collecting or using email addresses, screen names or other identifiers without the consent of the person identified (including, without limitation, phishing, Internet scamming, password robbery, spidering and harvesting);

1.6 collecting or using information without the consent of the owner of the information, including, but not limited to Internet scamming (tricking other people into releasing their passwords), password robbery, phishing, security hole scanning, and port scanning;

1.7 use of any false, misleading or deceptive TCP-IP packet header or any part of the header information in an e-mail or a newsgroup posting;

1.8 use of the Services to distribute software that covertly gathers information about a user or covertly transmits information about the user;

1.9 use of the Services for distribution of advertisement delivery software, unless:

(i) the user affirmatively consents to the download and installation of such software based on a clear and conspicuous notice of the nature of the software; and

(ii) the software is easily removable by use of standard tools for such purpose included on major operating systems (such as Microsoft's "add/removal" tool);

1.10 any activity or conduct that is likely to result in retaliation against Entity Data's network or website, or Entity Data's employees, officers, or other agents, including or engaging in behaviour that results in any server being the target of a Denial of Service attack (DoS);

1.11 any activity or conduct that is likely to be in breach of any applicable laws, codes or regulations including data protection;

1.12 introducing intentionally or knowingly into the Services any virus or other contaminating program or fail to use an up to date virus-scanning program on all material downloaded from the Services;

1.13 sending unsolicited e-mails ("spam");

1.14 misrepresenting yourself as other computer networks and users; or

1.15 any activity or conduct that unreasonably interferes with our other clients' use of our Services.

2. Bulk Commercial E-Mail

2.1 The use of e-mail for direct marketing is only allowed to recipients who have given their prior consent. We acknowledge that market research is not considered as direct marketing, and therefore, the requirements set out below don't apply to bulk e-mails for market research purposes. You must obtain our advance approval for any bulk commercial e-mail other than for market research purposes, for which you must be able to demonstrate the following to our reasonable satisfaction:

2.1.1 Your intended recipients have given their consent to receive e-mail via some affirmative means, such as an opt-in procedure;

2.1.2 Your procedures for soliciting consent include reasonable means to ensure that the person giving consent is the owner of the e-mail address for which the consent is given;

2.1.3 You retain evidence of the recipient's consent in a form that may be promptly produced within 72 hours of receipt of recipient's or our requests to produce such evidence;

2.1.4 The body of the e-mail must include information about where the e-mail address was obtained.

2.1.5 You have procedures in place that allow a recipient to revoke their consent.

2.1.6 You must post an abuse@yourdomain.com e-mail address on the first page of any Web site associated with the e-mail, you must register that address at abuse.net, and you must promptly respond to messages sent to that address;

2.1.7 You must have a privacy policy posted for each domain associated with the mailing;

2.1.8 You have the means to track anonymous complaints;

2.1.9 You must not obscure the source of your e-mail in any manner. Your e-mail must include the recipient's e-mail address in the body of the message or in the "TO" line of the e-mail;

2.1.10 You must not attempt to send any message to an email address if three (3) consecutive delivery rejections have occurred and the time between the third rejection and the first rejection is longer than fifteen (15) days.

2.1.11 You are complying with the "CAN-SPAM Act of 2003" governing commercial mailing.

2.2 These policies apply to messages sent using ENTITY DATA's network, or to messages sent from any network by you or any person on your behalf that directly or indirectly refer the recipient to a site hosted by ENTITY DATA. You may not use third party e-mail services that do not have similar procedures for all its customers. These requirements apply to distribution lists created by third parties to the same extent as if the list were created by you.

2.3 We may test and monitor your compliance with these requirements, including requesting opt-in information from a random sample of your list at any time.

3. Vulnerability Testing

You may not attempt to probe, scan, penetrate or test the vulnerability of an ENTITY DATA system or network or to breach ENTITY DATA's security or authentication measures, whether by passive or intrusive techniques without our prior written consent.

4. Newsgroup, Chat Forums, Other Networks

4.1 You must comply with the rules and conventions for postings to any bulletin board, chat group or other forum in which you participate, such as IRC and USENET groups including their rules for content and commercial postings. These groups usually prohibit the posting of off-topic commercial messages, or mass postings to multiple forums.

4.2 You must comply with the rules of any other network you access or participate in when using the Services.

5. Offensive Content

5.1 You may not publish, display or transmit via ENTITY DATA's network and equipment any content that we reasonably believe:

5.1.1 constitutes or encourages child pornography or is otherwise obscene, sexually explicit or morally repugnant;

5.1.2 is excessively violent, incites violence, threatens violence, or contains harassing content or hate speech;

5.1.3 is unfair or deceptive under the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes;

5.1.4 is defamatory or violates a person's privacy;

5.1.5 creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement bodies;

5.1.6 improperly exposes trade secrets or other confidential or proprietary information of another person;

5.1.7 is intended to assist others in defeating technical copyright protections;

5.1.8 infringes another person's trade or service mark, patent, or other property right;

5.1.9 is discriminatory in any way, including by way of sex, race, or age discrimination;

5.1.10 facilitates any activity or conduct that is or may be defamatory, pornographic, obscene, indecent, abusive, offensive or menacing;

5.1.11 involves theft, fraud, drug-trafficking, money laundering or terrorism;

5.1.12 is otherwise illegal or solicits conduct that is illegal under laws applicable to you or to us; and

5.1.13 is otherwise malicious, fraudulent, or may result in retaliation against us by offended viewers.

5.2 Content "published or transmitted" via our network or equipment includes Web content, e-mail, bulletin board postings, chat, and any other type of posting, display or transmission that relies on the Internet.

6. Copyrighted Material

6.1 You may not use ENTITY DATA's network or services to download, publish, distribute, or otherwise copy in any manner any text, music, software, art, image or other work protected by copyright law unless:

6.1.1 you have been expressly authorised by the owner of the copyright for the work to copy the work in that manner; and

6.1.2 you are otherwise permitted by copyright law to copy the work in that manner.

6.2 We may terminate the Services of copyright infringers in accordance with ENTITY DATA's Terms and Conditions.

7. Cooperation with Investigations and Legal Proceedings

7.1 We may monitor any content or traffic belonging to you or to users for the purposes of ensuring that the Services are used lawfully. We may intercept or block any content or traffic belonging to you or to users where Services are being used unlawfully or not in accordance with this AUP and you do not stop or provide us with an acceptable reason within 7 days of receipt of a formal written notice from us.

7.2 We may, without notice to you:

7.2.1 report to the appropriate authorities any conduct by you that we believe violates applicable law, and

7.2.2 provide any information we have about you, or your users or your traffic and cooperate in response to a formal or informal request from a law enforcement or regulatory agency investigating any such activity, or in response to a formal request in a civil action that on its face meets the requirements for such a request.

8. Shared Systems

You may not use any shared system provided by ENTITY DATA in a way that unnecessarily interferes with the normal operation of the shared system, or that consumes a disproportionate share of the resources of the system.

9. Other

9.1 You must have valid and current information on file with your domain name registrar for any domain hosted by ENTITY DATA.

9.2 You may only use IP addresses assigned to you by ENTITY DATA staff in connection with the Services.

9.3 You may not take any action which directly or indirectly results in any of our IP space being listed on any abuse database.

9.4 You may not operate any IRC (Internet Relay Chat) related services on the ENTITY DATA network, including; IRC servers, daemons, bouncers, bots, or clients. ALL IRC related activities are strictly forbidden.

9.5 You may not operate any game servers on the ENTITY DATA network under any circumstances. Game servers are strictly forbidden.

10. Consequences of Violation of AUP

You are strictly responsible for the use of the Services in breach of this AUP, including use by your customers, and including unauthorised use that you could not have prevented. We will charge you our standard hourly rate for work on any breach of the AUP together with the cost of equipment and material needed to:

10.1 investigate or otherwise respond to any suspected violation of this AUP;

10.2 remedy any harm caused to us or any of our customers by the use of your Services in violation of this AUP;

10.3 respond to complaints; and

10.4 have our Internet Protocol numbers removed from any "blacklist".

11. Disclaimer

We are under no duty, and by this AUP are not deemed to undertake a duty, to monitor or police our customers' activities and we disclaim any responsibility for any misuse of our network.

12. SLA

No credit will be available under your Service Level Agreement for interruptions of service resulting from AUP violations.