



Acceptable Use Policy

This Acceptable Use Policy outlines the types of activities that are not acceptable on the ForLinux network. All customers of ForLinux Network or Services must comply with this Acceptable Use Policy (AUP). Any failure to comply with the policy may lead to the termination of the contract of services, in accordance with the clauses set out in that contract.

ForLinux reserves the right to change this policy from time to time to reflect any changes in the law, regulation or community standards, or whenever it is deemed necessary by ForLinux to do so. Any changes to this policy will be effective upon posting to the ForLinux website www.forlinux.co.uk, or other such primary domain as may be notified to the customer in writing from time to time, and it will be the customer's responsibility to ensure that they are fully aware of these changes.

This AUP forms part of your contract with ForLinux and as such, any failure to comply with this policy may lead to the termination of the contract of services, in accordance with the clauses set out in that contract.

1. Illegal Use

The ForLinux Network and Services may be used for lawful purposes only and in compliance with all current and future statutes in force from time to time.

The Customer agrees not to use any of the contracted Services to store, send or receive materials or data which is

1.1 in violation of any laws or regulations. Examples of unlawful material include, but are not limited to the following:

- i) direct threats of physical harm
- ii) hardcore pornography
- iii) child sexual abuse content

1.2 defamatory, offensive, abusive, indecent or obscene

1.3 in breach of confidence, privacy, trade secrets

1.4 in breach of any third party Intellectual Property rights, including copyrighted, trademarked and other proprietary material without proper authority.

2. Violations of System or Network Security

Any violations of systems or network security are prohibited, and may result in the customer facing criminal and civil liability. ForLinux will investigate incidents involving such violations and will inform and co-operate with the relevant law enforcement organisations if a criminal violation is suspected.

2.1 Examples of such violations may include, but are not limited to the following:





- i) Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network
- ii) Unauthorised monitoring of data or traffic on any network or system without express authorisation of the owner of the system or network
- iii) Interfering with any user, host or network including mail bombing, flooding, deliberate attempts to overload a system, and broadcast attacks.

2.2 You may not store or distribute certain other types of prohibited material. Examples of prohibited material include, but are not limited to the following:

- i) programs containing viruses
- ii) Trojan horses and tools to compromise the security of other sites.

2.3 You may not run “scanning” software which accesses remote machines or networks, without the explicit permission of the owners of those remote machines or networks.

3. Email Usage

We will investigate complaints regarding e-mail and may take action based on the rules set out below. If an e-mail message is found to violate one of the policies below, or to contain unlawful material, as described in Clause 1 above, we may take action as outlined in Clause 7 below.

3.1 You may not send e-mail to any user who does not wish to receive it, either at ForLinux or elsewhere. We recognise that e-mail is an informal medium, however, users must refrain from sending further e-mail to a user after receiving a request to Opt-out.

3.2 Unsolicited advertising mailings, whether commercial or informational, are strictly prohibited. You may send advertising material only to addresses that have specifically requested it. We will not forward mail of accounts terminated for bulk mailing or unsolicited advertising.

3.3 Chain letters are unsolicited by definition and may not be propagated using our services.

3.4 You may not send, distribute, or reply to mail bombs. Mail bombing is defined as either e-mailing copies of a single message to many users, or sending large or multiple files or messages to a single user with malicious intent.

3.5 You may not use false email headers or alter the headers of e-mail messages to conceal their e-mail address or to prevent Internet users from responding to messages. You must not use any email address that you are not authorised to use.

Violations of the AUP outlined in this document can sometimes result in massive numbers of e-mail responses. If our users receive so much e-mail that our resources are affected, we may shut down a user's account.

ForLinux adhere to the ISPA guidelines for bulk unsolicited mail. This guidelines can be viewed in full at www.ispa.org.uk





4. World Wide Web (WWW)

4.1 You are solely responsible for the content of Web pages owned and/or operated by you.

4.2 We reserve the right to remove any Web page at any time and for any reason. We will investigate complaints regarding inappropriate material within Web pages on the ForLinux Network and may, at our own discretion, require that the material be removed or take action as outlined in Clause 7 below.

4.3 You may not use World Wide Web pages within or outside our domain to violate any part of the AUP, or to attempt to disrupt the pages or Internet experiences of other users.

4.4 Users whose web pages are generating excess traffic may receive a warning from us. Continued excessive use may result in termination of the contract of services, or additional charges, in accordance with the clauses in that contract.

5. Use of Internet relay Chat (IRC) or Video Conferencing

We do not monitor IRC channels. Any user in IRC may create a channel and hold operator privileges, and any user with operator privileges on a channel may remove anyone else from that channel. Channel operators are not our agents, and are in no way compensated or supervised by us, accordingly, we are not liable for the content of any communication made on IRC.

5.1 We will respond to complains of inappropriate behaviour in IRC. If the user's behaviour is found to violate any of our IRC policies, or to involve unlawful material, as described in Clause 1 above, we may take action as outlined in Clause 7 below.

5.2 Examples of inappropriate behaviour includes, but is not limited to the following:

- i) Users may not engage in "flooding". Flooding is understood as deliberately repeating actions in quick succession in order to fill the screens of other users with text.
- ii) Users may not maintain more than 3 simultaneous IRC connections from one account. This includes the use of automated programs, "bots" and "clones". A "bot" is a program written by a user to automatically execute IRC commands. Each bot counts as one IRC connection. You may run bots as long as the total number of connections does not exceed 3, and the bots do not violate any of our IRC guidelines. Bots may not be run while the owner is not logged in.
- iii) A "flash" is a message, which contains control code information designed to disrupt a user's terminal emulation or session. You may not send or relay such messages via any medium, including IRC.
- iv) One or more users with operator privileges or "ops", control each IRC channel. The holder of ops on a channel has the ability to remove any other user from that channel, temporarily or for as long as the channel exists. "Hacking" is defined as manipulation of IRC servers in order to harass or disconnect other users, or forcible seizure of ops on a channel for purposes of disruption or harassment. You may not engage in hacking or attempt to gain operator privileges for a channel without the permission of the current holder(s) of ops (if any) on that channel.





- v) As stated above, the holder of ops on a channel has the right to remove any users he or she considers offensive. Users who are removed have the option to move to another channel or create a channel of their own, where they hold operator privileges. You may not attempt to return to a channel after being banned from it.
- vi) Any user has the ability to screen out messages from a user that they find objectionable, using the "ignore" command. You may not attempt to continue sending private messages to a user after being ignored.
- vii) You may adopt any available nickname for use in IRC, however, the "whois" command can be used to discover the username and hostname of any IRC user. You may not attempt to disguise your username or hostname in order to impersonate other users or to use IRC anonymously.

6. Investigation

ForLinux Ltd reserves the right to investigate suspected violations of this AUP. When we become aware of possible violations, we may initiate an investigation, which may include gathering information from the user involved and the complaining party, if any, and examination of material on our servers. Much of the AUP reflects acts that may constitute breaches of United Kingdom legislation or regulations and may in some cases carry criminal liability.

6.1 During an investigation, we may suspend the provision of service and/or connection to the network.

6.2 ForLinux are not required to notify the customer in advance of action being taken in response to any actual or suspected violation, where or not notified to ForLinux by a 3rd party.

6.3 ForLinux will determine what action will be taken in response to any violation on a case-by-case basis.

6.4 The customer acknowledges that ForLinux may be required by current or future law or regulation, including but not limited to the Regulatory of Investigatory Powers Act 2000, to access, monitor, store, take copies of, or otherwise deal with the Customer's data stored on or transmitted by the Service. Without limitation, you expressly authorise us to use your personal data and other account information in connection with any such investigation, including disclosing this data and account information to any third party authority that we consider has a legitimate interest in any such investigation or its outcome.

6.5 ForLinux reserves the right to terminate the Service with immediate effect and without further obligation or liability to the Customers as required by any law enforcement organisation or by the Courts.

7. Regulation of Investigatory Powers (RIP) ACT

ForLinux will take action to comply with the provisions contained in the RIP Act and any regulations enacted under it and shall fully co-operate with the UK authorities empowered under the Act.





8. Internet watch Foundation

ForLinux subscribe to and shall abide by advice given by the independent industry body, the Internet Watch Foundation ("IWF") in relation to content of the Internet. For further information regarding IWF and its policy, please refer to <http://www.iwf.org.uk>

9. Complaints

We have in place a procedure for handling your complaints about material stored and/or accessed via our service. If you wish to make such a complaint, please ensure that you make your complaint by email to abuse@ForLinux.co.uk. If you do not use this facility, we cannot guarantee that your complaint will be dealt with promptly.

10. Disclaimer

ForLinux are under no obligation, and by this AUP are not deemed responsible for monitoring or policing our customers' activities. ForLinux disclaim any responsibility for any misuse of our network.

