

Acceptable Use Policy

Ordered Data, Voice or Mobile Services may not be used in any manner, or to facilitate conduct, that is illegal, discriminatory, abusive, insulting, threatening, obscene, harassing, racist, or otherwise inappropriate. You or users of the Services commissioning, authorising, aiding, abetting, encouraging or inciting any person to use or attempting to use the Services in any such manner (including, but not limited to, by any one or more of the following acts) is strictly prohibited:

1. violation of all or any legal rights of any person in any jurisdiction is strictly prohibited;
2. using the Services in relation to crimes such as theft and fraud is strictly prohibited;
3. using the Services in breach of laws relating to the protection of copyright, trade secrets, patents or other intellectual property rights and laws relating to spam or privacy and whether such violation is by way of the installation or distribution of "pirated" software or otherwise, is strictly prohibited;
4. unauthorised copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music or video and the installation of any copyrighted software for which the Customer does not have an active license is strictly prohibited;
5. exporting software, technical information, encryption software or technology, in violation of domestic export control laws, is strictly prohibited;
6. introduction of malicious programs into our or our suppliers' networks or servers (e.g., viruses, worms, Trojan horses, e-mail bombs) is strictly prohibited;
7. revealing a Customer's account password to others or allowing use of, modification of or tampering with the Services by third parties is strictly prohibited;
8. using another person's name, username or password or otherwise attempting to gain access to the Services of any other person is strictly prohibited;
9. using the Services to actively engage in procuring or transmitting material that is in violation of sexual harassment or workplace relations laws is strictly prohibited;
10. effecting security breaches or disruptions of network communication is strictly prohibited. Security breaches include, but are not limited to, accessing data of which a Customer is not an intended recipient or logging into a server or account that the Customer is not expressly authorised to access or corrupting any data. For the purposes of this paragraph, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
11. port scanning or security scanning is strictly prohibited (where such scanning is carried out without our prior written authorisation);
12. circumventing user authentication or security of any of our or our suppliers' hosts, networks or account is strictly prohibited;
13. using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, any persons' terminal session, via any means, locally or via the Internet, is strictly prohibited;
14. sending unsolicited messages in breach of the *Spam Act 2003* is strictly prohibited;
15. any form of harassment, whether through language, frequency, or size of messages is strictly prohibited;
16. unauthorised use, or forging, of email header information is strictly prohibited;
17. solicitation of email for any email address, with the intent to harass or to collect replies is strictly prohibited;
18. creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is strictly prohibited;
19. use of the Services in breach of any person's privacy (such as by way of identity theft or "phishing") is strictly prohibited.
20. We may terminate any Services Contract if any Customer or user of the Services:
 - 20.1. infringes our Acceptable Use Policy or any Security Policy and our suppliers terminate any Upstream Supplier Service as a result;
 - 20.2. repeatedly infringes our Acceptable Use Policy or any Security Policy; or
 - 20.3. commits a material breach of our Acceptable Use Policy or any Security Policy.
21. You indemnify us in respect of any loss, costs or damage we incur as a result of any Customer's or user's breach of our Acceptable Use Policy or any Security Policy.