onecom

Acceptable Use Policy

1 General

1.1 This Acceptable Use Policy defines the acceptable use of Products.

1.2 In this Acceptable Use Policy, terms that are capitalised but not defined in this Acceptable Use Policy have the meaning set out in the Contract.

1.3 In this Acceptable Use Policy, **Software** means any software made available to the Customer by Onecom as part of the Products, including Third Party Software and any software owned by or licensed to Onecom.

1.4 Onecom may update this Acceptable Use Policy from time to time, so the Customer:

1.4.1 should check Onecom's website regularly at https://www.onecom.co.uk/terms-and-conditions/ for updates; and

1.4.2 acknowledges that continued use of the Products after any change will mean the Customer has accepted the updated version of the Acceptable Use Policy.

1.5 The Customer will be responsible and remain fully liable for use of the Products and any breach of the Acceptable Use Policy by Users.

1.6 A breach of this Acceptable Use Policy constitutes a breach of the Contract and may result in suspension or termination of the Products in accordance with the Contract.

2 Use of Products

The Customer will not (whether actually or attempted, directly or indirectly) use the Products to effect or participate in any of the following activities:

2.1 Message or Content Abuse

2.1.1 Sending or publishing unsolicited bulk messages, content, posts or communications in any form ("spam") or maintaining an open SMTP relay.

2.1.2 Producing content that may be regarded as:

(a) harmful to others, or Onecom's operation or reputation;

(b) contrary to a commercial agreement (e.g. breach of a non-disclosure obligation);

(c) abusive;

(d) obscene;

(e) deceptive;

(f) a nuisance;

(g) fraudulent;

(h) the creation or distribution of 'deepfakes' or other synthetic media intended to deceive;

(i) the non-consensual replication of any identifiable living individual's voice using AI or voice synthesis technology, whether for the purpose of impersonation, harassment, or deception;

(j) the systematic spread of misinformation or harmful disinformation; or

(k) content that harasses, threatens, intimidates, or discriminates against any individual or group on the basis of race, ethnicity, national origin, sex, gender, gender identity, sexual orientation, religious affiliation, age, disability, or any other protected characteristic.

2.2 Security or Network Abuse

2.2.1 Falsifying user or other service-related information, including omitting, deleting, forging or misrepresenting transmission information provided to Onecom; including headers, return mailing, Internet protocol addresses or any other part of a message describing its origin or route.

2.2.2 Withholding or cloaking the Customer's identity, origin or contact information, including assuming a sender's identity without the sender's explicit permission.

2.2.3 Accessing or threatening the integrity or security of any device, network or computer system, without proper authorisation; including, transmission of worms, viruses or other malicious codes.

2.2.4 Using any part of the Products with the intention of adversely affecting the operation or users of any computer system or network (including the Internet); including, denial of service attacks, web page defacement, port and network scanning, and unauthorised system penetrations; provided that these prohibitions shall not apply to activities conducted strictly within the scope of authorised security assessment services provided by Onecom (such as 'PenX'), where such activities are performed against authorised systems.

2.2.5 Using or permitting anyone to use the Products other than as expressly authorised by Onecom.

2.2.6 Merging or using the Equipment with any other hardware, software, products or services other than as expressly authorised by Onecom.

2.2.7 In respect of security testing services, the Customer must not use the Products to perform scanning, penetration testing, or exploitation against any systems, IP addresses, or applications for which they do not have explicit, written legal authorisation.

2.3 Harmful, Deceptive or Illegal Activities

2.3.1 Violating any law or regulation (including, libel, slander, invasion of privacy, harassment, obscenity, child sexual abuse material, export laws and regulations, and infringement or misappropriation of another party's copyrights, trademarks, patents, trade secrets or other intellectual property rights).

2.3.2 Engaging in other activities that degrade or interfere with users of the Products or other connected services.

2.3.3 Avoiding incurring charges in a way that is inconsistent with good faith commercial practice.

2.3.4 Using the Products for the purposes of unauthorised cryptocurrency mining or any other activity that places an excessive or disproportionate load on Onecom's (or its suppliers') infrastructure.

2.3.5 Use of AI or voice synthesis capabilities to impersonate any electoral candidate, generate misleading content about electoral processes, or conduct voter suppression through automated communications.

2.4 Spending Limits

In relation to relevant Services, spending more in Variable Charges than the applicable spending limits as set out in the Price Guide from time to time.

3 Use of Software

3.1 In relation to Software, the Customer will (whether actually or attempted, directly or indirectly):

3.1.1 not copy, reverse engineer, decompile, modify, disassemble, or otherwise attempt to derive the source or object code of Software; and

3.1.2 use Software in strict accordance with any instructions or software licence or other third party terms communicated or made available by Onecom or its suppliers from time to time.

3.2 In relation to AI-enabled Products or automated communication capabilities, the Customer shall:

3.2.1 not attempt to 'prompt inject' or otherwise manipulate AI logic to bypass security filters;

3.2.2 not use the Products to develop, train, or improve any machine learning or AI model, whether or not in competition with Onecom or any Third Party Service Provider;

3.2.3 not use automated tools to 'scrape' or harvest data from Onecom's portals or interfaces;

3.2.4 not use AI voice or speech synthesis capabilities to impersonate any individual without that individual's explicit consent, or to generate synthetic voice content designed to deceive any person about the identity of the speaker or the AI-generated nature of the content;

3.2.5 ensure that individuals interacting with such capabilities are informed of their AI-generated or automated nature;

3.2.6 not use AI-enabled Products to provide tailored professional advice (including (without limitation) medical, legal, financial, or psychological advice) without maintaining a qualified professional in the loop; and

3.2.7 not configure or permit any AI-enabled Product in a manner that solicits or encourages individuals interacting with the Product to share their passwords, full payment card details (including primary account numbers, CVVs, or expiry dates), bank account details, or other security credentials.