Business Acceptable Use Policy

Welcome to The One Broadband. We are committed to providing you with the best full fibre broadband experience possible. To keep our network running smoothly and ensure everyone enjoys a fast, reliable, and secure internet connection, we have a Business Acceptable Use Policy (AUP). Our business AUP sets out the rules for using our services. It's designed to protect you, our network, and the broader online community. By understanding and following these guidelines, you help us maintain a high quality service for everyone. Let's keep the internet a safe, fair, and enjoyable space for all our users. By using The One Broadband services, you agree to comply with this AUP. This policy is designed to ensure that our services are used in a lawful, ethical, and responsible manner, in compliance with UK Ofcom regulations. This policy may change from time to time, so please check back from time to time so that you are aware of any changes. We will seek to ensure that significant changes will be notified to you.

1. Introduction and scope

1.1 This Acceptable Use Policy ("AUP") sets out the standards of conduct expected of customers, end users, and any other person using internet access and connectivity services provided by The One ("The One", "we", "us", or "our").

1.2 This AUP applies to all business customers of The One' connectivity services. By using any such service, the customer agrees to comply with this AUP and to procure that all of its end users, employees, agents, and any other person using the service through the customer's connection (together, "Users") also comply with it.

1.3 This AUP forms part of the agreement between The One and the customer (the "Agreement"). In the event of conflict between this AUP and the main body of the Agreement, the main body of the Agreement shall prevail unless this AUP expressly states otherwise.

1.4 Defined terms used in this AUP have the meanings given in the Master Services Agreement, save for any terms defined in this AUP.

1.5 This AUP does not apply to web hosting, application hosting, email hosting, or other hosted services provided by The One. Those services are governed by the separate Hosting Acceptable Use Policy.

2. Summary of customer obligations

2.1 In summary, customers and Users must:

(a) use the service only for lawful purposes;

(b) not interfere with, or attempt to interfere with, the operation of The One' network or any other network or system;

(c) not engage in activity that compromises the security or integrity of The One' network, third-party systems, or other customers;

(d) respect the rights of others, including intellectual property rights, privacy rights, and rights against harassment;

(e) comply with all applicable laws and regulatory obligations, including those identified in clause 3;

(f) cooperate with The One in investigating any incident or alleged breach of this AUP; and

(g) comply with the technical, routing, security, and email use rules set out in the remainder of this AUP.

3. Compliance with applicable laws

3.1 Customers and Users must comply with all laws applicable to their use of the service. Without limitation, this includes:

(a) the Computer Misuse Act 1990;

(b) the Communications Act 2003 (including section 127);

(c) the Malicious Communications Act 1988;

(d) the Public Order Act 1986 (Parts 3 and 3A relating to incitement to hatred);

(e) the Protection of Children Act 1978 and the Criminal Justice Act 1988 (relating to indecent images of children);

(f) the Online Safety Act 2023, where applicable to services the customer provides over the connection;

(g) the Copyright, Designs and Patents Act 1988;

(h) the Trade Marks Act 1994;

(i) the Data Protection Act 2018 and the UK GDPR;

(j) the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR");

(k) the Fraud Act 2006;

(l) the Equality Act 2010;

(m) the Terrorism Act 2000 and the Counter-Terrorism and Border Security Act 2019; and

(n) any other UK or international law applicable to the customer's or User's activities.

3.2 Where the customer makes the service, or any part of it, available to its own customers or end users, the customer remains responsible for compliance by those persons and is not relieved of any obligation under this AUP by reason of any contractual arrangement with them.

4. Prohibited use — general

4.1 Customers and Users must not use the service for any purpose, or in any manner, that:

(a) is illegal, including any of the activities prohibited by the laws referred to in clause 3.1;

(b) is fraudulent, deceptive, or designed to mislead;

(c) infringes the intellectual property rights of any person, including by unauthorised distribution of copyrighted material;

(d) is defamatory of any person;

(e) is obscene, grossly offensive, harassing, threatening, or abusive;

(f) incites violence or hatred on grounds of race, religion, sex, sexual orientation, gender identity, disability, or any other protected characteristic;

(g) constitutes or facilitates the creation, possession, or distribution of indecent images of children, or material promoting terrorism;

(h) creates a risk to the safety, health, or welfare of any person; or

(i) encourages or assists any person to do any of the above.

5. Network integrity, routing, and addressing

5.1 IP address allocation and assignment

5.1.1 Where The One allocates or assigns Internet Protocol ("IP") addresses to the customer, those addresses remain the property of, or under the administrative control of, The One or the relevant Regional Internet Registry ("RIR") at all times.

5.1.2 The customer's right to use any IP address allocated by The One is conditional on its compliance with this AUP and the Agreement, and ceases automatically on termination of the relevant service.

5.1.3 Customers must not announce, route, or otherwise use any IP address space that has not been allocated to them by The One, by an RIR, or by another lawful holder of the address space who has authorised such use.

5.1.4 Reverse DNS for IP addresses allocated by The One may be delegated on request, subject to The One' standard processes. The customer is responsible for ensuring that any reverse DNS records configured under such delegation are accurate and not misleading.

5.2 BGP routing (where applicable)

5.2.1 This clause 5.2 applies where the customer establishes a Border Gateway Protocol ("BGP") session with The One.

5.2.2 Customers must announce to The One only IP prefixes that:

(a) have been allocated to the customer by The One; or

(b) are held by the customer or a downstream entity for which the customer has documented routing authorisation; and

(c) are covered by valid Route Origin Authorisations ("ROAs") where the customer maintains Resource Public Key Infrastructure ("RPKI") authority over the relevant prefixes.

5.2.3 Customers must:

(a) maintain accurate route objects in the relevant Internet Routing Registry ("IRR");

(b) update prefix lists, AS-SETs, and ROAs promptly when routing changes;

(c) implement appropriate inbound and outbound BGP filters to prevent the propagation of bogus, leaked, or hijacked routes;

(d) not announce more-specific prefixes for the purpose of avoiding filtering or for any other improper purpose;

(e) not engage in route hijacking, prefix squatting, or any deliberate misrouting; and

(f) cooperate with The One in any investigation of routing incidents.

5.3 Anti-spoofing and source address validation

5.3.1 Customers must implement source address validation in accordance with BCP 38 (RFC 2827) and BCP 84 (RFC 3704), or equivalent measures appropriate to their network architecture, to prevent the transmission of packets with forged source IP addresses from their network onto the The One network.

5.3.2 Customers must not transmit, or knowingly permit the transmission of, packets with forged source IP addresses, forged MAC addresses, or other forged or impersonated identifiers.

5.4 Denial of service and amplification

5.4.1 Customers and Users must not engage in, participate in, or knowingly facilitate any denial-of-service attack, distributed denial-of-service attack, amplification attack, reflection attack, or similar activity directed at The One, any other customer, or any third party.

5.4.2 Customers must take reasonable steps to prevent their network and connected systems from being used (whether knowingly or unknowingly) to participate in such attacks. This includes, where appropriate:

(a) patching or mitigating known UDP amplification vectors (including DNS open resolvers, NTP monlist, SSDP, Memcached, Chargen, and similar);

(b) rate-limiting outbound traffic where appropriate;

(c) monitoring for unusual outbound traffic; and

(d) promptly remediating any compromised system identified.

5.5 Interference with the network

5.5.1 Customers and Users must not, and must not attempt to:

(a) interfere with, disrupt, or impair the operation of The One' network or any equipment, system, or service forming part of it;

(b) circumvent, evade, or overcome any access control, rate limit, traffic management measure, security measure, or filter implemented on the network;

(c) monitor, intercept, or capture data or traffic on the network without authorisation;

(d) introduce malicious code, viruses, worms, trojans, ransomware, or other harmful software or instructions onto the network or any connected system; or

(e) engage in any activity reasonably likely to cause excessive load on, or impair the performance of, the network.

6. Security and unauthorised access

6.1 Customers and Users must not, without the express written authorisation of the owner of the relevant system or network:

(a) access, attempt to access, or use any computer, system, network, account, or data;

(b) probe, scan, or test the vulnerability of any computer, system, or network, including by port scanning, vulnerability scanning, fingerprinting, or penetration testing;

(c) attempt to circumvent or breach any authentication, access control, or security mechanism;

(d) obtain, attempt to obtain, or use credentials belonging to another person; or

(e) engage in any activity that constitutes an offence under the Computer Misuse Act 1990.

6.2 Customers must take reasonable security measures in respect of their own equipment and systems connected to the service, including:

(a) maintaining current security patches on operating systems and software;

(b) implementing appropriate authentication and access controls;

(c) running supported endpoint protection where appropriate;

(d) securing the customer's wireless networks (where applicable) with industry-standard encryption and strong credentials; and

(e) promptly remediating any known compromise.

6.3 Customers must promptly notify The One via the abuse contact in clause 11 on becoming aware of:

(a) any actual or suspected compromise of any system or device connected to the service;

(b) any actual or suspected compromise of credentials issued by The One;

(c) any unauthorised use of the service or of IP addresses allocated by The One; and

(d) any other security incident affecting the service or originating from the customer's network.

6.4 The One may, on becoming aware of a security incident affecting or originating from the customer's connection, take reasonable measures to protect the network, other customers, and third parties, including the temporary filtering, rate-limiting, or suspension of the customer's connection. The One shall notify the customer of any such action as soon as reasonably practicable.

7. Email and electronic messaging

7.1 Customers and Users must not:

(a) send any email, instant message, SMS, or similar communication that contravenes PECR, the UK GDPR, the Data Protection Act 2018, or any other applicable law;

(b) send unsolicited commercial communications to any person who has not given prior consent or to whom such communications cannot lawfully be sent under PECR;

(c) operate any open SMTP relay or other open mail forwarder accessible from the public internet;

(d) forge, falsify, alter, or otherwise misrepresent the headers or routing information of any email or electronic message, including the sender address, return path, or any other identifying information;

(e) send email or electronic messages of a harassing, threatening, or abusive nature; or

(f) engage in mail-bombing, list-bombing, or any similar high-volume abuse of email.

7.2 Customers operating their own mail infrastructure must implement appropriate sender authentication for outbound mail, including SPF, DKIM, and DMARC, and shall publish accurate records for the domains used.

7.3 The One may impose reasonable rate limits, throttling, or filtering on outbound mail traffic to protect the network and the reputation of its IP address space. Where such measures are imposed in response to a specific customer or User, The One shall notify the customer.

7.4 If any IP address allocated by The One to the customer is listed on a third-party blocklist as a result of activity originating from the customer's connection, the customer shall cooperate with The One in remediation and de-listing efforts. The One may decline to seek de-listing where the underlying activity has not been remediated.

8. Content transmitted over the service

8.1 The One operates as a provider of internet access. It does not actively monitor, filter, or moderate content transmitted over the service, save where required to do so by law or where necessary to enforce this AUP, protect the network, or respond to a security incident.

8.2 The customer is responsible for content transmitted by the customer or any User over the service, and for the lawfulness of any service the customer makes available over the connection.

8.3 Customers must not use the service to publish, transmit, store, or distribute content that:

(a) constitutes indecent images of children, or content otherwise unlawful under the Protection of Children Act 1978 or the Criminal Justice Act 1988;

(b) promotes terrorism or terrorist organisations contrary to the Terrorism Act 2000 or the Counter-Terrorism and Border Security Act 2019;

(c) incites violence or hatred contrary to the Public Order Act 1986;

(d) is unlawful under any of the laws referred to in clause 3.1; or

(e) is otherwise prohibited under clause 4.1.

8.4 The One works with the Internet Watch Foundation ("IWF") and other recognised bodies in the identification and removal of indecent images of children. Customers must cooperate with any IWF notice or other lawful takedown notice received in respect of content originating from the customer's connection or service.

8.5 Where the customer hosts user-to-user content or operates a service in scope of the Online Safety Act 2023, the customer remains solely responsible for compliance with its own duties under that Act.

9. Lawful disclosure, retention, and cooperation with authorities

9.1 The One is a public electronic communications network and service provider regulated under the Communications Act 2003. As such, it may be required, or authorised, to:

(a) intercept communications under a warrant issued under the Investigatory Powers Act 2016;

(b) acquire, retain, or disclose communications data under the Investigatory Powers Act 2016;

(c) comply with technical capability notices, retention notices, or other instruments issued under that Act;

(d) comply with court orders, production orders, regulatory notices, or other lawful demands;

(e) respond to lawful requests from law enforcement and regulatory authorities; and

(f) cooperate with the National Crime Agency, GCHQ, the police, Ofcom, the Information Commissioner's Office, and other competent bodies.

9.2 The One shall comply with all such requirements and shall not be in breach of any duty of confidentiality owed to the customer by reason of any disclosure, interception, or retention required or permitted by law.

9.3 Where lawful and operationally practicable, The One shall notify the customer of any disclosure made under clause 9.1. Where The One is prohibited by law from notifying the customer, no such notification shall be given.

9.4 The customer must cooperate with The One in responding to any lawful request affecting the customer's service, account, or connection, including by providing such information and assistance as may be required.

10. End users and downstream customers

10.1 Where the customer makes the service, or any part of it, available to its own customers, end users, or any other person, the customer shall:

(a) ensure that each such person is bound by terms substantially equivalent to this AUP;

(b) remain primarily responsible to The One for compliance with this AUP by all such persons;
(c) maintain accurate records of the identity of such persons sufficient to enable identification of the source of any incident;
(d) promptly action any abuse report or notification from The One affecting such persons; and
(e) promptly suspend or terminate the connection of any such person who breaches this AUP and continues to do so following written notice from the customer.

10.2 The One may require the customer to provide evidence of compliance with clause 10.1 on reasonable request.

11. Abuse reporting and contact

11.1 Reports of abuse, security incidents, copyright infringement notices, or other matters arising under this AUP should be sent to:

Email: abuse@theonebroadband.co.uk

Postal: Abuse Team, 85 Great Portland Street, First Floor, London, England, W1W 7LT

Out-of-hours emergencies: Helpdesk

11.2 The One aims to acknowledge abuse reports within one (1) Business Day of receipt and to provide a substantive initial response within five (5) Business Days. Response times for serious incidents (including those involving illegality, ongoing security threats, or imminent harm) will be substantially shorter.

11.3 Customers must publish their own abuse contact details, conforming to RFC 2142 (i.e. an abuse@ address for each domain operated), and must monitor and respond to messages sent to that address.

11.4 Customers must keep their administrative, technical, and abuse contact details current with The One. The One may rely on the contact details most recently notified by the customer.

12. Enforcement, suspension, and termination

12.1 The One may take any of the following actions in response to a breach of this AUP, having regard to the nature and seriousness of the breach:
(a) issue a written warning to the customer;
(b) require the customer to remedy the breach within a specified time;
(c) filter, rate-limit, or otherwise traffic-manage the customer's connection;
(d) suspend the customer's service or any part of it;
(e) terminate the customer's service in accordance with the Agreement;
(f) report the matter to law enforcement or other competent authorities;
(g) withdraw the use of any IP addresses or other resources allocated to the customer; and
(h) claim damages or any other remedy available at law or under the Agreement.

12.2 The One shall ordinarily provide the customer with written notice and a reasonable opportunity to remedy a breach before taking action under clauses 12.1(c) to 12.1(e), save where:
(a) the breach involves illegality;
(b) the breach poses an imminent threat to the security or integrity of the network, to other customers, or to third parties;
(c) The One is required to act immediately by law or by lawful instruction; or
(d) the customer has previously been notified of similar conduct.

12.3 In any case described in clause 12.2(a) to 12.2(d), The One may act without prior notice and shall notify the customer of the action taken as soon as reasonably practicable thereafter.

12.4 Suspension or termination under this clause 12 does not relieve the customer of any obligation to pay charges accrued up to the date of suspension or termination. The customer may be charged for the reasonable costs of investigating and remediating any breach of this AUP.

13. Indemnity

13.1 The customer shall indemnify The One on demand against all liabilities, costs, expenses, damages, losses, and reasonable legal fees suffered or incurred by The One arising out of or in connection with:

(a) any breach of this AUP by the customer or any User;

(b) any claim by a third party arising from the customer's or any User's use of the service; or

(c) any failure by the customer to comply with applicable law in connection with the use of the service.

13.2 Any liability cap or limitation in the Master Services Agreement does not apply to liability under clause 13.1 to the extent it relates to (i) illegality, (ii) breach of clause 5.4 (denial of service), (iii) breach of clause 6 (security), or (iv) breach of clause 8.3 (prohibited content).

14. Changes to this AUP

14.1 The One may amend this AUP from time to time. Material changes will take effect 30 days after notice is given to the customer or the updated AUP is published on The One' website, whichever is earlier.

14.2 Where The One makes a change to this AUP that is materially adverse to the customer, and the customer is a Microenterprise within the meaning of Ofcom General Condition C1, the customer may terminate the affected service without penalty by written notice given before the change takes effect.

14.3 Non-material changes (including changes to abuse contact details, regulatory references following changes in law, clarifications, and corrections) may take effect immediately on publication.

14.4 The current version of this AUP is the version published on the The One website. Earlier versions are retained for reference and are available on request.

15. Interpretation

15.1 Headings are for convenience only and do not affect interpretation.

15.2 References to laws or statutory provisions include any consolidation, re-enactment, modification, or replacement, and any subordinate legislation.

15.3 References to a person include a body corporate, partnership, unincorporated association, trust, and any other entity, and include that person's successors and permitted assigns.

15.4 The words "include", "including", and "in particular" are illustrative and do not limit the sense of the words preceding them.

15.5 References to clauses are to clauses of this AUP unless otherwise stated.

15.6 This AUP is governed by the laws of England and Wales. The courts of England and Wales have exclusive jurisdiction over any dispute arising out of or in connection with it.

ACCEPTABLE USE POLICY

Internet Access and Connectivity Services

Document title	Business Acceptable Use Policy — Internet Access and Connectivity Services
Document owner	The One
Version	1.0
Effective date	28.04.26
Last reviewed	28.04.26
Applies to	All customers of The One's business connectivity services, including leased line, broadband, ethernet access, IP transit, IP allocations, and any other service involving Internet access or use of the The One IP network.