

Acceptable Use Policy

Version 2.0 | Effective from 1 September 2026 | www.rocket-fibre.co.uk

1. About this policy

1.1 This policy sets out how the services provided by Rocket Fibre Ltd (registered number 12821973, registered office Unit 5 Perth House, Corby Gate Business Park, Corby, Northamptonshire, NN17 5JG) may and may not be used. In this policy “we”, “us” and “our” mean Rocket Fibre Ltd, trading as Rocket Fibre; “you” means the account holder; and “the services” means our broadband, telephone and mobile services, our website and our customer portal.

1.2 The policy forms part of your contract with us. For residential customers it is incorporated by clause 1.2.4 of our Residential Terms and Conditions, which also explain, in clauses 7, 8, 11 and 12, what we may do if it is breached. Business, wholesale and colocation customers are bound by it through their own contracts, and section 12 explains how it applies to them. Words defined in the Terms and Conditions have the same meaning here.

1.3 Its purpose is simple: to make sure that the way one customer uses the services does not harm other customers, our network, or anyone else. Almost everything people do online is unaffected by it. It exists for the small number of cases where a connection is used to break the law, to attack or abuse others, or to put the network at risk.

2. Your responsibility for your connection

2.1 You are responsible for all use of the services from your premises, whether by you, your household, your guests or anyone else you allow to use them, and for any use made through your equipment or account details if you have not kept them secure. Please make sure that everyone who uses your connection knows what this policy requires.

2.2 Keep your Wi-Fi protected by a strong password, keep the Router and your own devices updated, and keep your portal login and account security answers private. If you think your Wi-Fi, a device or your account has been compromised, or that someone else is using your connection without permission, tell us straight away and we will help you secure it.

2.3 Residential services are provided for your personal, domestic use at your premises. You must not resell or re-supply them, share your connection with people outside your household on a commercial basis, or use them to run a business, as clause 2.2 of the Terms and Conditions explains; if you need a service for business use, we will be glad to provide one on business terms.

2.4 Parental controls are available at your request, free of charge, to help you manage what can be accessed over your connection; they are described in our Traffic Management Policy. Responsibility for what children in your household see and do online remains with you.

3. What you must not do

You must not use the services, or allow them to be used:

3.1 Unlawfully. For any purpose that is a criminal offence, fraudulent, or otherwise unlawful, or in a way that breaches any law or regulation that applies to you or to us.

3.2 To harm others. To send, publish, store or make available material that is defamatory, obscene, indecent, menacing, abusive, harassing, discriminatory, or that incites hatred or violence; to threaten, stalk or harass anyone; or to send messages that are grossly offensive or that are intended to cause distress or anxiety, which is an offence under the Communications Act 2003 and the Malicious Communications Act 1988.

3.3 For illegal content. To access, store, send or distribute child sexual abuse material, terrorist material, or any other content that is illegal to possess or distribute. We report such use to the police and to the Internet Watch Foundation, and we cooperate fully with any investigation.

3.4 To infringe rights. To copy, share, store or distribute material in breach of copyright, trade marks or other intellectual property rights, including the unauthorised sharing of films, music, games, software, broadcasts or books; or to breach anyone's privacy or data protection rights, or a duty of confidence.

3.5 To deceive. To send messages or make calls that misrepresent who you are, that forge headers, calling line identity or other origin information, or that are part of a scam, phishing attempt or other fraud.

3.6 To damage the network or other customers. In a way that degrades or interferes with the services received by other customers, puts our network or the Infrastructure Provider's network at risk, or is not reasonably expected of residential use, as described in sections 4 to 7.

3.7 To damage our reputation. In a way that brings us into disrepute, for example by generating complaints from other networks or organisations, or by causing our addresses to be listed as sources of abuse.

4. Network security and abuse

4.1 You must not, and must not attempt to: gain unauthorised access to any computer, network, account or data; probe, scan or test the vulnerability of any system without the express permission of its owner; intercept or monitor data or traffic that is not intended for you; launch, take part in or facilitate a denial of service attack; distribute, control or host malware, viruses or botnets; send traffic with forged source addresses; run open mail relays, open DNS resolvers or other services that can be used to reflect or amplify attacks; or evade or interfere with any security, monitoring or traffic management measure we use.

4.2 A device on your connection that has been compromised, for example by malware, can attack others without your knowledge. If we detect that, we will contact you and ask you to fix it; if the risk to others is serious we may restrict or suspend the connection first and contact you as soon as we have done so, and we will restore it once the device has been secured. Our Traffic Management Policy explains the security measures we apply to the network.

4.3 The Computer Misuse Act 1990 makes unauthorised access to, and interference with, computers and networks a criminal offence. We will report offences to the police where appropriate and will disclose information about your account to

public authorities where the law requires or permits, as our Privacy Policy explains.

5. Email, messaging and spam

5.1 You must not send unsolicited bulk or commercial email, text or other messages (spam), including marketing messages that breach the Privacy and Electronic Communications (EC Directive) Regulations 2003; send chain letters or hoaxes; send excessive volumes of messages to disrupt a service or mailbox; harvest addresses or details for those purposes; or use the services to sell or promote the sending of spam by others.

5.2 Where we provide an email service, mailboxes and sending limits are set to protect the service from abuse, and messages that our systems identify as spam or malware may be filtered or rejected. You should not rely on an email account as the only copy of anything important.

6. Telephone services

6.1 Inclusive and unlimited call allowances on the Voice Services are for your personal, residential use. Clause 6.6 of the Terms and Conditions sets out the fair use rules, including the point at which unusually heavy use, such as more than 1,000 inclusive minutes in a month or individual calls of more than 60 minutes, may indicate non-residential use and what we may do about it.

6.2 You must not use the Voice Services for telemarketing, call centre operations, automated or auto-dialled calling, continuous call forwarding, resale or revenue generation, or to generate artificially inflated traffic; make hoax, nuisance, silent or abusive calls, including to the emergency services; present a calling line identity that you are not entitled to use or that misleads the person you are calling; or make calls that breach the Telephone Preference Service rules. Ofcom's rules on calling line identity and nuisance calls apply to any use you make of the service for calling others.

7. Servers, hosting and sharing your connection

7.1 You may run equipment and services on your connection for your own personal, domestic use, such as a home storage device, a games server for friends or a camera you view remotely, provided they are kept secure and do not breach section 4. Unless you take a static IP address as an Additional Service your connection has a shared, dynamic address, which limits what can be reached from outside; our Traffic Management Policy explains this.

7.2 You must not use a residential service to host websites, applications or services for the public or for commercial purposes, to provide services to third parties, or to operate a network, Wi-Fi service or hotspot for people outside your household, whether or not you charge for it. Business services are available for all of these.

7.3 Any device or service you run must not generate abuse reports, be listed as a source of spam or attacks, or be left open for others to misuse. If it is, section 11 applies.

8. Copyright notices and legal requests

8.1 Rights holders monitor file-sharing networks and send notices to internet providers identifying the connection involved. If we receive a notice that relates to your connection we may pass it on to you so that you can deal with it, and repeated notices about the same connection will be treated as a breach of this policy. We do not hand over your details to a

rights holder unless a court orders us to, as our Privacy Policy explains.

8.2 We may be required by a court order or by law to block access to particular websites or services, and to retain and disclose information about your connection to public authorities under the Investigatory Powers Act 2016. Our Privacy Policy and Traffic Management Policy explain when this happens and what it means for you.

9. Content and services that are not ours

9.1 The websites, services and content you reach through the services are provided by others. We are not responsible for their accuracy, availability, legality or security, and you use them at your own risk and on their terms. Where we block access to material under a legal requirement or to protect the network, clause 16.4 of the Terms and Conditions applies.

9.2 You must use our website and portal lawfully, give us accurate information through them, and not attempt to disrupt them, gain unauthorised access to them, or extract information from them by automated means.

10. Reporting abuse

10.1 If you believe that one of our customers, or a connection on our network, is being used in breach of this policy, please tell us at abuse@rocket-fibre.co.uk. Include the date and time, with time zone, the IP addresses involved, and any logs, message headers or other evidence you have. We acknowledge abuse reports and investigate them, and we tell the reporter what we have done where we can do so without disclosing another customer's personal data. Requests from law enforcement and public authorities should be sent to the same address and are handled as our Privacy Policy describes.

10.2 If you believe a website or service you can reach through your connection contains illegal content, report it to the police and, for child sexual abuse material, to the Internet Watch Foundation at report.iwf.org.uk. Please also let us know.

11. How we enforce this policy

11.1 We investigate suspected breaches of this policy, whether we detect them ourselves or they are reported to us, and we act reasonably and fairly in doing so, as clause 7.3 of the Terms and Conditions requires. We take the least step that will deal with the problem, taking into account how serious the breach is, whether it is deliberate, whether it has happened before, and the harm or risk to others.

11.2 Depending on the breach, the steps we may take are: contacting you to explain the problem and asking you to put it right within a stated time; a formal warning; blocking the traffic, port, service or content involved; suspending some or all of the services; ending your contract under clause 12.1 of the Terms and Conditions, in which case any Cancellation Charge for the remainder of your minimum period applies; and reporting the matter to the police or another authority where we are required to or consider it appropriate. We may also charge you our reasonable costs of investigating and dealing with the misuse, as clause 7.3 provides, and you are responsible under clause 18 for losses we suffer as a result of misuse of the services.

11.3 We will normally give you the chance to put things right before we suspend a service. We may act first, and tell you afterwards, where the breach is serious, for example an attack on others, the distribution of illegal content, fraud, or a continuing risk to the network or to other customers, or where the law requires it. Charges continue during a suspension caused by your breach, and we restore the service, at our discretion under clause 7.4, once the cause has been put right.

11.4 If you disagree with a step we have taken you can complain under our Complaints Code of Practice, which for residential and small business customers includes the right to take an unresolved complaint to the Communications Ombudsman.

12. Business, wholesale and colocation customers

12.1 Business broadband customers may use the services for their business, and sections 2.3 and 7.2 do not apply to them; everything else in this policy does, and it applies to their staff, customers and anyone else using their connection.

12.2 Wholesale, carrier, transit and colocation customers are responsible for making sure that their own customers and end users comply with sections 3 to 9. They must publish and staff a working abuse contact, respond to abuse reports we forward within one working day, act on them promptly, and take down or disconnect a source of abuse when we reasonably require it. They must announce only address space they are authorised to announce, and not originate or relay traffic with forged source addresses. Where their contract with us,

including the Master Services Agreement, sets out specific abuse handling, service level or suspension provisions, those provisions take precedence over section 11.

13. Changes to this policy

13.1 We may update this policy under clause 19 of the Terms and Conditions. A change that is not to your benefit, is not purely administrative and is not required by law will be notified to you at least 30 days before it takes effect, and you may end your contract without a Cancellation Charge if you do not accept it. The version number and effective date are shown at the top, and the current version is always published on our website.

13.2 Version history. Version 1.0, 15 March 2025: original policy. Version 2.0, 1 September 2026: rewritten to align with the Residential Terms and Conditions version 3.0 and the Traffic Management Policy, to remove the usage restriction and the separate indemnity, to set out a proportionate enforcement process, and to cover telephone services, home servers, copyright notices, abuse reporting and wholesale customers.