

The following Fair Usage Policy list details all the uses of ResQ IT & Telecom's ("ResQ") Internet services that we consider unacceptable or 'unfair' usage. ResQ maintains and promotes a policy of fair and acceptable usage at all times, so please ensure that any use of ResQ 's services, by yourself or anyone in your household or office doesn't in any way contradict the restrictions listed below. You will also find your responsibilities to help keep our network secure listed at the end of this Fair and acceptable usage policy (the 'Policy').

Please ensure that anyone using your account to access ResQ's Internet services agrees with this Policy and is aware of their obligations under it. This extends to your children or members of your household or your employees or office workers or any one accessing the network through your home or office.

ResQ's Internet Services Cannot be used for:

1. Unlawful, fraudulent, criminal or otherwise illegal activities
2. Sending, receiving, publishing, posting, distributing, disseminating, encouraging the receipt of, uploading, downloading, recording, reviewing, streaming or using any material which is offensive, abusive, defamatory, indecent, obscene, unlawful, harassing or menacing or a breach of the copyright, trademark, intellectual property, confidence, privacy or any other rights of any person
3. Commercial purposes, unless you are a customer who is working from home as a sole trader in business on your own account or a Business Customer, in which case see below for limits on certain types of commercial use)
4. Sending or uploading unsolicited emails, advertising or promotional materials, offering to sell any goods or services, or conducting or forwarding surveys, contests or chain letters except that ResQ customers working from home as a sole trader in business on their own account or business customers are permitted to send marketing communications in accordance with the Privacy and Electronic Communications Regulations 2003 if sent in batches of no more than fifty (50) emails at any time, each individual campaign being sent to no more than five hundred (500) recipients, with no more than five (5) campaigns per month
5. Knowingly or negligently transmitting or uploading any electronic material (including, without limit, files that contain viruses, corrupted files, or any other similar software or programmes) which is known or likely to cause, interrupt, damage, destroy or limit the functionality of any computer software, hardware or telecommunications equipment owned by ResQ or any other Internet user or person
6. Activities that invade another's privacy, cause annoyance, inconvenience or needless anxiety to any person
7. Activities that are in breach of any other third party's rights, including downloading, installation or distribution of pirated software or other inappropriately licensed software, deletion of any author attributions, legal notices or proprietary designations or labels in any file that is uploaded, falsification of the origin or source of any software or other material
8. Anything that may disrupt or interfere with ResQ's network or services or cause a host or the network to crash

IRG Computers Ltd / ResQ IT & Telecoms Internet Fair Usage Policy 2011 v1

ResQ IT & Telecoms Ltd Unit 14 Cross Hands Business Workshops, Cross Hands, Llanelli, SA14 6RE

Tel: 01269 500055 email info@resq.co.uk

9. Launching "denial of service" attacks; "mailbombing" attacks; or "flooding" attacks against a host or network
10. Granting access to your ResQ services to others not residing at or located at the premises at which these Internet services are provided
11. Making excessive use of, or placing unusual burdens on, the network, for example by sending or receiving large volumes of email or excessively large email attachments
12. Circumventing the user authentication or security process of a host or network
13. Creating, transmitting, storing or publishing any virus, Trojan, corrupting programme or corrupted data
14. Monitoring or recording the actions of any person entitled to be in your home or business premises without their knowledge or any person or thing outside of your home or premises including, without limitation, any public highway or roadway or another person's home or business premises
15. Collecting, streaming, distributing or accessing any material that you know, or reasonably should know, cannot be legally collected, streamed, distributed or accessed.

Security

You are responsible for ensuring that any member ID and/or password selected by you remains confidential and all connection equipment secure, so that the network cannot be used by any unauthorised person.

The member ID and/or password referred to includes, but are not limited to, those controlling access to (a) any computer hardware systems or networks; (b) any computer software or applications; or (c) any other services accessed by you in the use of either of the above.

You shall not disclose any member ID or password to any third party, or use the same for any purpose connected with the improper use of the network including accessing or attempting to access other parts of the services for which you do not have access rights.

You are responsible for taking all reasonable steps necessary to prevent a third party obtaining access to the network.

You must immediately advise us if you become aware of any violation or suspected violation of these Security provisions.

What about usage by kids and others without you knowing?

You are responsible for all uses made of ResQ 's Internet services through your account (whether authorised or unauthorised) and for any breach of this Policy whether an unacceptable use occurs or is attempted, whether you knew or should have known about it, whether or not you carried out or attempted the unacceptable use alone, contributed to or acted with others or allowed any unacceptable use to occur by omission. You agree that ResQ are not responsible for any of your activities in using the network. Although

the Internet is designed to appeal to a broad audience, it's your responsibility to determine whether any of the content accessed via ResQ 's Internet service is appropriate for children or others in your household or office to view or use.

Spam

Spam is illegal in the EU and often carry viruses or links to websites which promote fraud. ResQ reserves the right to block any emails that have the characteristics of spam. You'll be contacted by ResQ if any emails sent by you are blocked for this reason. Any spamming activity may result in suspension or termination of your service at ResQ 's option and sole discretion.

Excessive network usage

If it's felt that any ResQ member's Internet activities are so excessive that other members are detrimentally affected, ResQ may give the member generating the excessive web traffic a written warning (by email or otherwise). In extreme circumstances, should the levels of activity not immediately decrease after the warning, ResQ may terminate that member's services.

Excessive traffic can be the result of viruses, in these instances an IP address may be blacklisted (often out of our control), connections may be restricted or even terminated to protect the network until the customer equipment has been cleaned from viruses or malware.

What happens if the Policy is breached?

If any member's use of these services constitute a breach of this Policy, ResQ may, at its option and discretion, either give the member notice to stop the unacceptable use(s) or terminate that member's services (with or without notice as ResQ considers appropriate).

ResQ supports, and is in the process of becoming a member of, the Internet Watch Foundation (IWF). The IWF is the UK hotline for the public to report potentially illegal website content relating to child abuse, together with material of an unlawful nature. For more information about the IWF and its services please visit <http://www.iwf.org.uk>.

To report any illegal or unacceptable use of ResQ services, please send an email to abuse@resq.co.uk.