Acceptable Use Policy: Telecoms Services

This Policy is intended for the information and guidance of Customers, and forms part of the SCC Master Service Agreement. The purpose of this Policy is to outline those actions which are either strictly prohibited or are considered unacceptable by SCC in particular or by the Internet Community in general, whether they be committed willfully, inadvertently or innocently, and to define the sanctions which may be imposed by SCC upon Customers in violation of this Policy.

SCC places no obligation upon itself to monitor any traffic, website or other information transmitted on or stored within its network. However, SCC will fully investigate all complaints received concerning use of the network in contravention of this Policy and will co-operate fully with law enforcement agencies where criminal violation is suspected.

The Customer shall use all best endeavours to comply with all obligations contained in herein and be responsible for ensuring that all users of the service shall be aware of this Policy. The Customer shall further be responsible for ensuring that these regulations are complied with at all times, and acknowledges that any violation of these regulations by the users of the Service supplied to the Customer by way of trade or otherwise may give rise to liability, whether civil or criminal.

The integrity and security of the SCC network is necessarily of prime importance, and any action that adversely affects, or threatens to adversely affect, the operation of the network is strictly prohibited under this Policy. Insofar as the SCC network is linked with other Networks that form the Internet as a whole, this shall include any such action against any other network.

Users must not under any circumstances whatsoever commit, or attempt to commit, nor aid nor abet any action that may threaten the network, either deliberately, negligently or innocently; this shall include but is not limited to:

- any attempt to crash a host or network,
- “denial of service” attacks, “mailbombing” attacks or “flooding” attacks against a host or network
- any attempt to circumvent the user authentication or security of a host or network
- any profligate use of the network, including the sending of IP multicast other than by means provided by and coordinated by SCC, the sending of excessively large attachments other than by using file transfer protocol,
- the creation, transmission, storage, or publication of any kind of virus or corrupting program or corrupted data,
- any other action that may adversely affect the network or its operation,
- continuous use of a service which breaches fair usage allowances, or negatively affects other users, or negatively affects SCC.

SCC shall have the right to suspend or terminate Service, and to take such defensive action as may at SCC’s sole discretion be deemed necessary in the event of any attack upon the network. Furthermore, SCC will instigate Civil and/or Criminal Proceedings as appropriate against the perpetrators of such prohibited action.

For the purposes of this Policy;

“Illegal Activities” shall be construed so as to include any act or omission by the Customer that

would constitute a criminal offence or any act or omission that could give rise to legal action whether under the laws of contract, tort or otherwise. You should be aware that as the internet is a global network, some activities/material which may be legal in the UK, may be illegal elsewhere in the world and vice versa.

“Unlimited” relates to services with an unlimited data or call package. The reasonable allowance is defined by each network’s own Acceptable Usage Policy which is available on request.

Violation of any of the provisions herein may constitute a civil or criminal offence and is **strictly prohibited** under this policy.

USERS

Users shall not commit, attempt to commit, nor aid nor abet the transmission, storage, publication or use of any of the following:

- Material that is illegal to possess including but not limited to:
- child pornography,
- web pages whose purpose is to provide links to child pornography,
- material subject to the Official Secrets Acts.
- Users who receive unsolicited material in the above category should report this immediately to SCC, and then remove it from their machine. Not to do so may itself constitute a criminal offence.
- Material that is legal to possess but illegal or unacceptable to publish or transmit, including but not limited to:
- articles of an obscene or offensive nature,
- articles likely to encourage conduct of a criminal or otherwise illegal nature,
- articles of a libellous or slanderous nature,
- articles of a racist nature,
- articles that are hateful or abusive in any manner,
- articles that are unlawful in any manner,
- copies of software obtained by unauthorised means.

In the event that a complaint is received in respect of such violation, SCC may immediately suspend or terminate access to the relevant website, and report the matter to the relevant UK Police authority and the Internet Watch Foundation. Copies of the offending material and any upload logs held will be made for evidential purposes and passed to the authorities; all further copies will then be destroyed by whatever means are available. SCC will co-operate to the fullest extent in any resultant investigation.

In recognition of the fact that users of the Internet should be entitled to such use without interference from third parties, SCC will not permit any action which would violate this right, whether directed against an individual user, a group of users or indiscriminately. Users will not commit, attempt to commit, nor aid nor abet any of the following, nor transmit, store, publish or use software or tools for the purpose of any of the following:

- “spamming” i.e. sending of, or collecting responses from
- bulk e-mail,
- “scanning” i.e. probing for security weaknesses in another user’s systems, “denial of service” or “mailbombing” attacks, i.e. a deliberate attempt to overload a network or machine,
- “hacking” and/or “cracking” i.e. unauthorised access to or use of another user’s network or machine,
- unauthorised monitoring of other users,
- “port scanning”
- cancellation, interception, alteration, redirection or unauthorised publication of other user’s messages
- soliciting e-mail for another user’s address
- generating credit card details whether with intent to defraud, or for any other unlawful use,
- the propagation or forwarding of petitions for signature, chain letters or pyramid schemes,
- the unauthorised use, alteration or destruction of other user’s data or passwords,
- the creation or transmission of any kind of virus or corrupting program or corrupted data whether wilful, inadvertent or innocent; a user who receives such a virus should report this immediately by telephone to their Service Provider
- any other action that would compromise or interfere with the normal functioning of another user,
- any other action that would violate the privacy of another user.

In the event that a complaint is received in respect of any of the above violations, SCC shall have the right to:

- order that the offending software or tools be destroyed
- require a written undertaking that the User shall not re-offend
- restrict or suspend access to the Service provided until such time as these requirements are complied with.

If a satisfactory response is not received within twenty-four (24) hours of notification of such violation, then SCC shall have the right to terminate the Services at SCC’s sole discretion.

MAIL

The sending of unsolicited bulk e-mail (also known as UBE, JunkMail or Spam), including political or religious tracts, or unsolicited commercial e-mail (also known as UCE), is considered an unacceptable use of the Service. It interferes with the operation of the Internet as a whole by creating congestion which delays and blocks legitimate traffic, contributing to the general degradation of service, and creating unwanted traffic for recipients. Where the

User has acquired explicit permission, either on a website or through some other relationship the User should keep a record of this permission and must cease sending e-mail when requested to stop.

Users must ensure that they do not further the sending of unsolicited bulk e-mail by others. This applies to both material that originates on the User's system and also to third party material that may pass through it. This includes but is not limited to a prohibition on running an "open mail relay" which will accept e-mail from unauthorised or unknown senders and will forward it to a destination outside of the User's machine or network. If the User's machine does relay mail, on an authorised basis, then it must record its passing through the User's system by means of an appropriate "received" line.

In order to act in the best interest of Internet users, SCC is committed to ensuring that such general abuse of the Internet is kept to an absolute minimum, and will investigate fully all reports of such abuse. SCC at its discretion may run manual or automatic systems to determine the user's compliance with these provisions, including scanning for open mail relays. The user by entering into an Agreement with SCC has granted permission for this limited intrusion into the user's network.

Users may run an anonymous relay service where this anonymity can reasonably be required for legitimate purposes, provided that the User monitors this service in such a way as to detect and prevent unauthorised or excessive use.

SCC will fully investigate all reports of violations. For this purpose Users must ensure that a standards compliant "received" line is added to all e-mail that passes through their systems. In the event that a complaint is received in respect of such violation, SCC shall be entitled to:

- request that equipment which is not standards compliant be replaced or reconfigured so as to prevent further recurrence of the violation and,
- require a written undertaking that the User shall not re-offend and,
- suspend access to the Service provided until such time as these requirements are complied with.

If a satisfactory response is not received within five (5) working days of notification of such violation, then SCC shall have the right to terminate the Services at SCC's sole discretion.

COPYRIGHT

Violation of the laws regarding intellectual property rights constitutes a civil offence and is strictly prohibited under this policy. Users shall not commit, attempt to commit, nor aid nor abet the unauthorised transmission, storage, publication or use (unless it is "fair use" as defined by relevant legislation) of any of the following:

- Copyright material, including but not limited to software programs, research documents and works of literature.
- Trademarks, including but not limited to brand names, logos and product names, and including signs identical with or similar to a registered mark.
- Intellectual property of any other kind including, but not limited to, trade secrets or patents.

In the event that a complaint is received in respect of such violation, SCC shall be entitled to

request either:

- Evidence that the Customer is the legal owner of the intellectual property, or
- Evidence that the Customer has authority to use the intellectual property from the legal owner, or
- An explanation of why a “due cause” exemption should apply, or
- A written undertaking to remove the material and to desist from such action in the future.

If a satisfactory response is not received within five (5) working days of notification of the violation, SCC shall have the right to restrict, suspend or terminate access to the facility at SCC’s sole discretion, and to refer the infringement to the legal owner.

VISIBILITY

SCC recognises that users of the Internet have a right to privacy, and that there are situations where it is desirable or necessary that anonymity be preserved. It is not intended to remove or to erode these rights but to ensure that anonymity is available where and when appropriate, and that it is not used to invade the privacy of other users. Accordingly, unless there is an exemption agreed in writing by SCC, the user may not under any circumstances conceal, alter or forge, nor attempt to conceal, alter or forge any information pertaining to their electronic identity, which action includes but is not limited to:

- “spoofing” i.e. sending e-mail from an e-mail address which is not the User’s own address.
- “forging” i.e. concealing or amending or adding to the User’s e-mail address.
- “bouncing” i.e. deliberately exploiting insecure systems to avoid or attempt to avoid identification of the User’s address.

SCC reserves the right to modify or make additions to this Policy at any time, and these variations shall be effective upon publication of the revised Acceptable Use Policy on SCC’s website. The decision of SCC in respect of any matter under the provisions contained within this Policy shall be final.

SCC subscribe to and shall abide by the advice given by the independent industry body The Internet Watch Foundation (“IWF”) in relation to the content of the Internet. For further information regarding IWF and its policy please refer to http://www.internetwatch.org.uk

Complaints regarding any Illegal or Unacceptable use should be sent to telecoms@scc.com