COUNSEL'S CHAMBERS LIMITED

P: +61 2 9231 3644
E: admin@ccl.com.au
W: www.ccl.com.au
A.B.N. 72 000 111 302

Level 1 Selborne Chambers
174 Phillip Street Sydney
NSW 2000 Australia
DX: 973 Sydney

Connection of Personal Router to the CCL Network

Router Policy v1.1, 25 July 2017

Name of owner/user of Router: _____

Email address: _____

Chambers: _____

Router Model: _____

Router Mode: ◯ Bridged ◯ Routed

MAC address: _____

(Enter End-Device (PC) address for Bridged mode or Router address for Routed mode)

By signing below you:

i. Agree to the terms of the attached Acceptable Use Policy, Wireless Network Connections Policy and other policies that may be in force or changed from time to time; and
ii. Indemnify CCL and users of the CCL Network against any damage, loss and malicious activity or other breach of these policies arising from the installation and/or use of the personal router.

Signed: _____ Date: _____

COUNSEL'S CHAMBERS LIMITED

P: +61 2 9231 3644
E: admin@ccl.com.au
W: www.ccl.com.au
A.B.N. 72 000 111 302

Level 1 Selborne Chambers
174 Phillip Street Sydney
NSW 2000 Australia
DX: 973 Sydney

Rev 2.3 08 May 2017

CCL's Acceptable Use Policy
Policy for the use of CCL Network

APPLICATION

1. This policy sets out terms and conditions on which *User*s may access and use *CCL*'s Network. Please read this document carefully before accessing *CCL*'s Network.

2. This policy applies to all *User*s of the *CCL Network*. Each *User* acknowledges and agrees that the terms and conditions of this policy are fair and reasonable and further acknowledges and agrees that access and use of the *CCL Network* has been and is being provided by *CCL* at no additional cost to the *User*.

3. By using *CCL*'s Network, each *User* agrees to comply with the terms of this policy and further acknowledges and agrees that a failure to comply with this policy may lead to suspension or termination of the *User*'s access to and use of *CCL*'s Network.

4. This policy should be read together with the *Other Network Policies* which are also binding on *User*s. All current terms and conditions and policy documents which are binding on *CCL Network User*s are published on the *CCL* website: www.ccl.com.au

5. For the avoidance of doubt, all *CCL Network User*s must at all times comply with the Macquarie Telecom Services Agreement Acceptable Use Policy as amended from time to time by Macquarie Telecom. The version which is current and applicable as at the date of this policy can be found at: https://macquarietelecom.com/service-agreements/

DEFINITIONS

CCL	means Counsel's Chambers Limited;
CCL Network	means the internet (both cable and wireless), data, VoIP and related infrastructure and services provided by *CCL*;
CCL Services	means the services provided through the *CCL Network*;
other Network Policies	means and includes the: (a) Network (Data and VoIP) Connection Terms and Conditions dated 5 August 2015, (b) Policy for the Maintenance and Use of Communication and

	Network Services Infrastructure Rises dated 6 March 2007, (c) Network Interconnection Policy (Data VoIP) dated 6 March 2007, (d) Wireless Network Connections Policy dated 08 May 2017, as amended from time to time by *CCL* in its absolute discretion without notice to *User*s and also includes any other policies which *CCL* may in its absolute discretion issue in respect of use and access to the *CCL Network*;
Prohibited Internet Gambling Content	means content hosted by a prohibited Internet gambling service as defined by the Interactive Gambling Act 2001;
Prohibited Online Content	means Prohibited Content as defined by the Broadcasting Services Act 1992;
us or ***we***	means *CCL*;
user	means any person who has access to or uses the *CCL Network* including any of *CCL*'s members or their staff, *CCL*'s employees and contractors, and any other person who has been granted access to the *CCL Network*; and,
you or your	is a reference to any *User*.

CONDITIONS ON ACCESS AND USE OF THE CCL NETWORK

1. *CCL* reserves the right at any time to monitor the quantity of *your* usage of the *CCL Network* (ie, the amount of data downloaded and uploaded) and to ensure *you* are acting in compliance with this Policy.

2. *You* must ensure that *your* employees, agents, sub-contractors, clients and visitors comply with *CCL*'s Acceptable Use Policy if *you* permit or allow them to use the *CCL Network*. *You* must also ensure that *you* do not permit or allow a minor to use the *CCL Network* other than with express consent and supervision of their parent or guardian.

3. Without limiting the terms of use, *you* agree that the *CCL Network* may not be used in any manner that is not permitted under *CCL*'s Acceptable Use Policy or that is otherwise unlawful.

4. *You* must not:

(a) use the *CCL Network* to commit or engage in crimes including (but not limited to): theft and fraud, the publication and/or distribution of prohibited or potentially *Prohibited Online Content*, accessing *Prohibited Internet Gambling Content*;

(b) use the *CCL Network* to engage in breach of laws relating to the protection of copyright, trade secrets, patents or other intellectual property rights or in breach of laws relating to spam or privacy, whether such violation is by way of the installation or distribution of "pirated" software or otherwise;

(c) carry out unlawful copying of copyrighted material including, but not limited to, unlawful digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music or video and the installation of any copyrighted software for which *you* do not have an active license;

(d) export software, technical information, encryption software or technology, in violation of domestic export control laws;

(e) introduce malicious programs into the *CCL Network* or servers (e.g., viruses, worms, Trojan horses, e-mail bombs);

(f) except for a purpose which would not constitute a breach of *CCL*'s Acceptable Use Policy, reveal *your* account password to others (other than for a legitimate, honest and reasonable reason that is expressly authorised by *you*, such as to *your* secretary or an authorised delegate of *your*s);

(g) provide *your* account password to or otherwise assign or give control of *your* account to a minor, or provide *your* account password to others to permit use of, modification of or tampering with the *CCL Network* by third parties;

(h) except for a purpose which would not constitute a breach of *CCL*'s Acceptable Use Policy, use another person's name, username or password or otherwise attempt to gain access to the service of any other person (other than for a legitimate, honest and reasonable reason that is expressly authorised by that other person, such as where that person is *your* secretary or has authorised *you* to be their delegate);

(i) effect security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which *you* are not an intended recipient or logging into a server or account that *you* are not expressly authorised to access or corrupting any data. For the purposes of this paragraph, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;

(j) carry out Port scanning or security scanning (where such scanning is carried out without the prior written authorisation of *CCL*);

(k) execute any form of network monitoring which will intercept data not intended for *you*;

(l) circumvent *user* authentication or security of any *CCL* host, network or account;

(m) use any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, any persons' terminal session, via any means, locally or via the Internet;

(n) send unsolicited email messages in breach of the Spam Act 2003;

(o) carry out unauthorized use, or forging, of email header information;

(p) create or forward "chain letters", "Ponzi" or other "pyramid" schemes of any type;

(q) use the *CCL Network* in breach of any person's privacy (such as by way of identity theft or "phishing").

5. Because it is important that all *User*s of the *CCL Network* are able to access the *CCL Network* at all times, *you* must limit *your* use to "fair use". *You* must:

(a) be cognisant of the fact that the *CCL Network* is shared services and act accordingly;

(b) ensure that *your* use of the *CCL Services* does not detrimentally impact on the use of the *CCL Network* by other *User*s;

(c) be at all times aware that *your* use of the *CCL Network* does not permit *you* to engage in "unlimited downloads" particularly at peak times; and

(d) be at all times aware that where one *user* is constantly downloading large files it will slow the connection for the other *user*s.

6. If *you* do not comply with the terms of this Acceptable Use Policy, *CCL* may contact *you* to discuss how *you* can change the way *you* use the *CCL Network* so as to comply with the terms of this Policy. If *you* thereafter continue to act in a manner which is not in conformity with any of the terms of this Policy, *CCL* may, without notice, terminate or suspend *your* use of and access to the *CCL Network*.

LIMITATIONS, WARRANTIES AND INDEMNITIES

1. *CCL* will at all times use reasonable endeavours to ensure the *CCL Services* are provided continuously and that they are adequate for the needs of *User*s.

2. *You* use the *CCL Network* at *your* own risk and *you* agree that *CCL* does not warrant to *you* that the *CCL Services*:

(a) will be available for use without any interruption; and

(b) are suitable or adequate for the purposes required by *CCL Network User*s.

3. In the event that the *CCL Services* are interrupted, suspended or otherwise fail to operate for any reason whatsoever for any period of time, *you* will not be entitled to claim from *CCL* any damages for any loss or liability of any nature whatsoever incurred by *you* or *your* employees, subcontractors or agents including in respect of any personal injury (including death), any loss of or damage to property or any economic loss incurred or suffered as a consequence of the interruption, cessation or failure of the *CCL Services*.

4. *You* will raise no objection to nor make any claim against *CCL* in relation to any action taken by, or agreement entered into, by *CCL* concerning the *CCL Services* which is required by law or Court order including in relation to the storage of any data stored by *you* on the *CCL Services*.

5. *You* acknowledge and agree that *CCL* does not warrant to *you* or any third parties that any data:

(a) stored on the *CCL Services*, or

(b) which is transmitted or communicated via the *CCL Services* and *CCL Network*, or

(c) the transmission or communication of which is being facilitated by the *CCL Services* and *CCL Network*,

including the contents of privileged legal advice (*Your* Data), will be preserved, not collated, not monitored or not accessed by third parties under the authority of any law or Court order or otherwise.

6. *You* further acknowledge and agree that *CCL* does not have any obligation to ensure that *Your* Data is not accessed, not collated and not monitored by third parties.

7. *You* must indemnify and hold harmless *CCL*, its officers, employees, agents, contractors and other *User*s from and against all loss, damage, costs (including reasonable legal costs and expenses) or liabilities including consequential loss that may be incurred, suffered or sustained by any or each of them as a direct or indirect result of:

(a) *your* breach of, or failure to comply with, any provision of *CCL*'s Acceptable Use Policy, the *Other Network Policies* or the Macquarie Telecom Services Agreement Acceptable Use Policy, as amended from time to time;

(b) any unlawful or negligent act, act or omission by *you* in *your* use of or access to the *CCL Network*;

(c) any unlawful or negligent act, act or omission by any person, who *you* have authorised, permitted or enabled to use the *CCL Network*, in the course of or in connection with that person's use of or access to the *CCL Network*.

COUNSEL'S CHAMBERS LIMITED

P: +61 2 9231 3644
E: admin@ccl.com.au
W: www.ccl.com.au
A.B.N. 72 000 111 302

Level 1 Selborne Chambers
174 Phillip Street Sydney
NSW 2000 Australia
DX: 973 Sydney

Rev 2.1 08 May 2017

CCL's Wireless Network Connections Policy

PURPOSE

The purpose of this document is for Counsel's Chambers Limited (CCL) to take measures to protect the Counsel's Chambers Data and VoIP Network ("the CCL Network"), and the users of the CCL Network from unauthorised access, malicious activity, either passive or active, from malicious attackers utilising wireless technologies.

SCOPE

The scope of this policy is to define the appropriate use of wireless networking technologies on any part of the CCL Network. This includes technologies such as but not limited to the IEEE 802.11 series of standards.

RATIONALE

The increasing prevalence of wireless technology can create major security holes within the CCL Network, giving unauthorised access to both user systems and networks. Most wireless technologies and devices are insecure by default, and many authentication and authorisation schemes that are widely used provide insufficient, if any, security.

POLICY

Installation

Installation of wireless devices to be connected to or which are able to access the CCL network must be first approved by CCL in writing and all installations maintenance must be performed by a CCL approved contractor. Approval can be granted upon application to Counsel's Chambers Limited. Approval is subject to a written undertaking to comply with this and all other policy documents published by CCL from time to time.

The owner/operator of the device must also sign the form provided by CCL which is attached to this Policy and marked 'A'. By the execution of this form the owner/operator of the device indemnifies CCL and the users of the CCL network against any damage or malicious activity arising from the installation or use of the wireless device.

Wireless access points may only be installed for the use by existing CCL Network users. Encryption keys or credentials must not be provided to third parties, including guest access and existing and new network users.

Minimum Security Requirements

All wireless devices must provide adequate authentication and authorisation of devices connecting to it, and must prevent all unauthorised access.

All data traversing the wireless link must be encrypted such that it is not possible for an unauthorised person or device to decrypt it.

Encryption keys must be changed on a regular basis and must meet minimum strength requirements.

The minimum approved standard for encryption will be revised from time to time.

WPA2 Personal is currently the minimum approved encryption standard.

WPA2 with authentication is the current recommended standard.

Personal Area Network (PAN) devices which use protocols such as Bluetooth and Infrared must use high levels of encryption where available, and should be disabled when not in use.

ENFORCEMENT

Any breach of this policy will result in the immediate disconnection from the CCL Network of the offending hardware without warning or notice. Any users of the CCL Network found in breach of this policy are liable to be denied further access to the CCL Network without notice.

The cut-off of services is not dependent upon any damage having been caused to the network or any user(s) of it, or infiltration occurring prior to the time of cut-off.

The cut-off is not in lieu of any damages which may be caused to the network or any user(s) and each user specifically absolves Counsel's Chambers Limited from any liability for any cut-off by the CCL Network in the circumstances listed in this section.

DEFINITIONS:

CCL Network: The computer, data and VoIP network including all hosts (computers, switches, hubs, routers, firewalls and other networking hardware) owned or operated by Counsel's Chambers Limited, and all devices connected by a wired or wireless connection to these.

Host: A piece of computer hardware which is connected to a network. This includes PCs, notebooks, smartphones, tablets, switches, routers, network printers, servers, wireless access points etc.

IEEE 802.11: The Institute of Electrical and Electronics Engineers, Inc (IEEE) is a global professional association, who develop and publish standards, particularly relating to technology and communications. The 802.11 family of standards defines the specifications for wireless LAN technology.

IP Network: A network of hosts, communicating on the Internet Protocol.

Malicious Activity: Any activity that compromises or potentially compromises the security, integrity and/or privacy of data residing on or moving through the CCL Network or the CCL Network itself or which denies access to or unreasonably slows the speed of the CCL Network and/or hosts residing on the CCL Network.

Network: Computer or data or VOIP network. This includes both wired and wireless networks.

Wireless Device: A piece of computer hardware that communicates with other devices using protocols including but not limited to IEEE802.11 ("Wi-Fi"), Bluetooth and IrDA (infrared).

WEP: Wired Equivalent Privacy, defined in the IEEE 802.11 standards in an attempt to facilitate secure wireless communications. This protocol has serious flaws and does not provide an adequate level of privacy, security, or data integrity

WPA: Wi-Fi Protected Access. This encryption scheme can use an 802.1 lx authentication server, or can use Pre-Shared Keys ("personal" mode). For this scheme to be secure, strong passwords must be used.

WPA2: Defined in IEEE 802.1 li, the currently recommended security standard. If using Pre-Shared Key mode, the password length must be at least 20 characters and not vulnerable to Dictionary Attacks.