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

CIRCULAR TO CCL SHAREHOLDERS, CLERKS AND NETWORK MEMBERS - CCL NETWORK - FULL DEPLOYMENT OF CISCO WI-FI SERVICE

Friday 11th May

I refer to my attached circular dated 27 March 2018 regarding the use of private routers on the CCL Network.

CCL is pleased to announce that it will undertake a full deployment of the CCL Network Cisco Wi-Fi service (which is currently only about 70% deployed), as described below, in Wentworth, Selborne, Windeyer and Lockhart Chambers over the coming months and all members of the CCL Network on CCL Member Floors will have full access to this service in the majority of areas throughout the buildings.

CCL has now completed its investigations as mentioned in the attached circular and, whilst it is not entirely clear if there are statutory breaches, the collection of metadata is only one of the issues associated with the connection of personal routers to the CCL Network, there are several serious security and support implications associated with permitting consumer routers (particularly wireless routers) to connect to the CCL Network, including:

- Low level security protocols (e.g. pre-shared key, including weak passwords which could be shared with or guessed by unauthorised people).
- Firmware is rarely or never updated.
- CCL has no visibility over who has access to the network through the router.
- Lack of strong authentication of the router, and connected devices, to the CCL network.
- Radio interference with the CCL wireless network.
- Additional support burden with incompatible devices.

Accordingly, it is unfortunately necessary to phase out the use of personal routers on the CCL Network.

CCL will no longer permit the connection of any new personal routers on its network and existing routers will need to be phased out over the next 12 months at which time they must be disconnected.

The following should be noted in relation to the full deployment:

- The installation of the access point devices will be based on a site survey which has been prepared by CCL's consultants.
- On floors where there has not already been a full deployment of the Wi-Fi service, CCL may add the additional access point devices.
- On floors that currently have a full deployment of the Wi-Fi service some of the access points in the corridors may be relocated to ensure optimal coverage.
- Floors will remain financially responsible for the Floor switches and connection of the Wi-Fi devices will be based on the Floor switch being able to facilitate the additional connections.

- On Floors where existing Wi-Fi equipment has reached end-of-life, the access points will be replaced.
- CCL will be responsible for payment of the ongoing annual maintenance of the Cisco Wi-Fi devices, as well replacement of the devices in the future at end-of-life.

CCL appreciates that not all Wi-Fi devices (both new and existing) can be connected to the Cisco Wi-Fi service which is a commercial grade Wi-Fi as distinct from most of the private routers which are currently connected and are mainly suitable for domestic use. Devices need to be compatible with WPA2-Enterprise protocols (this is common practice in commercial environments). CCL currently uses a certificate-based authentication known as EAP-TLS. Wi-Fi devices need to be able to connect using this type of authentication and devices that are not compatible with EAP-TLS authentication will no longer be supported on the CCL Wi-Fi Network. CCL IT staff have done a lot of work in this area over recent months and we are confident that all current versions of Windows, OSX, IOS and Android devices are compatible. For devices that do not support WPA2-Enterprise authentication we have found a solution that will allow a number of commonly used devices (such as wireless printers) to connect and will be assessed on a case-by-case basis. CCL is currently considering expanding the authentication parameters to support password-based authentication. This system is much more widely supported, CCL will advise users further in this regard towards the end of the year. However, it is critical that, before purchasing new equipment for connection to the CCL Network, users check that the equipment is compatible with the above protocols and users should also check with their current equipment provider in relation to the compatibility of their current devices.

Please let me know if you have any questions in relation to the above. CCL IT Staff will in touch with Floor Clerks over the coming months to discuss installation on each of the Floors.

Kind regards,

Debbie George
General Manager

COUNSEL'S CHAMBERS LIMITED

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

P: +61 2 9231 3644
E: dgeorge@ccl.com.au
W: www.ccl.com.au