

Free Wireless Internet Access

Frequently Asked Questions

Q. Who can use the free-high-speed wireless Internet service?

The service is available to the entire court public; court agency and law enforcement partners, attorneys and staff.

Q. How fast is the high-speed wireless Internet service?

The court's wireless network provides access speed of 20 MBps for the public Internet.

Q. What devices may I use to access the wireless Internet service?

Personal data assistants (PDA), cell phones, and any 802.11b/g/n internet capable devices may be used.

Q. How do I access the court's wireless Internet service?

Most devices will automatically detect the wireless network. If this doesn't happen with your device try the following settings:

- SSID or Network Name: Court-public
- WEP/WPA/WPA2: Disabled
- TCP/IP Settings: DHCP Enabled or Obtain IP Address Automatically
- DNS: Obtain DNS Automatically via DHCP
- Default Gateway: Obtain Automatically via DHCP
- Network Mode: Infrastructure Only

Q. If I have trouble accessing the wireless network, who do I contact for assistance?

Contact your device manufacturer for assistance.

Q. Where can I find more information if I am a juror or prospective juror?

<http://www.saccourt.ca.gov/jury/jury.aspx>

Internet Use Policy

All wireless users must follow guidelines while using the court's wireless network.

Misuse of the wireless network may result in loss of wireless and Internet connectivity solely at the discretion of the Court, and may also be followed by a criminal investigation.

Misuse includes, but is not limited to using the wireless network for any illegal activity, sending spam, hacking into or causing damage to other local or Internet computing devices or resources, sending harassing messages to others, violating copyright and software licensing agreements, and viewing materials that are obscene or offending to others.

Blogging in the jury assembly room or while serving on a case in an assigned courtroom is strongly discouraged. If a juror is found to be blogging information in reference to a case they have been assigned to during trial, this would be a violation of the juror's oath.

Wireless Security

Although the court user and court guest wireless networks have security, the public wireless network is not and does not use any form of encryption or authentication mechanisms. A wireless network possesses all the security vulnerabilities that a wired network has. The most significant source of risks in wireless networks is the transmission media used, the airwave.

All wireless transmissions occur over the airwave and therefore are vulnerable to unauthorized disclosure of information, denial of service (DoS) attacks, and unauthorized access to name a few. The following two links provide more information regarding public wireless Internet usage and security. These links cover important information regarding the security of your computing device and the information flowing through your wireless connection. Please take the necessary precaution and educate yourself prior to using the wireless network.

Tips for Working Securely from Hotspots

<http://www.microsoft.com/atwork/remotely/hotspots.aspx>

Disclaimer

The court is not responsible for any changes you make to your computing device's settings as a result of attempting to connect to its wireless network. It is expected that the user or owner of the laptop, PDA, cell phone or other internet device is capable of configuring the wireless connection.