

Sydney Olympic Park Authority Policy

Policy Name SOPA Venues Internet Terms of Use Policy

Policy No. POL15/2

Department File No. SV15/199

Business Unit Sports Venues

Officer Responsible Manager Information Technology
SOPA

Approving Officer

Date of Approval

Version	Review	Date	Approved by
1		April 2015	

SOPA Venues Internet Terms of Use Policy

Purpose

SOPA Venues provide internet access to clients on a pre-arranged basis.

The objectives of this document are to provide guidance to clients concerning the SOPA policy requirements for client usage of SOPA supplied internet.

Definitions

Client – A Client is defined as any person or organisation requiring connectivity to SOPA supplied internet for event hosting requirements.

Employees – An Employee is defined as any SOPA or SOPV staff member.

Systems – For the purposes of this policy, systems are any SOPA owned or managed computer systems or networks. This includes, but is not limited to:

- Workstations
- Servers
- Switches
- Firewalls
- Virtual Private Network Devices
- SOPA LAN/WAN
- Laptops or notebooks
- WIFI network and devices

Compliance

The Terms and Conditions of Hire requires the client to ensure that the client and the clients employees are aware of and comply with this policy.

Violations of this policy can lead to the following actions:

- Immediate termination of use of SOPA systems to all users associated with the clients event.
- Referral of misuse/unlawful activities to the relevant authorities where required by law.

Terms and Conditions of Hire agreement

This policy forms part of the Terms and Conditions of Hire agreement for the venue.

Legislation

Electronic documents and transmissions are subject to legislation such as the Government Information and Public Access Act 2009 and to legal processes such as discovery and subpoena.

Clients should have no reasonable expectation of privacy subject to the SOPA Privacy Management Plan, available for download at www.sopa.nsw.gov.au/privacy.

Quality of Service

SOPA cannot guarantee the speed and connectivity of the internet line provided. Where possible SOPA Venues may take reasonable steps to rectify any internet related issues.

Monitoring

Internet access is provided for the sole purpose of event operations, and as such, SOPA reserves the right to monitor and log all aspects of internet traffic. The content of electronic communications maybe monitored at any time without notice. The usage of electronic communications systems will also be monitored to support operation, maintenance, auditing, security and investigative activities.

SOPA logs, monitors, audits and reports on network and system activities. These tasks are performed for a number of reasons, which include but are not limited to:

- Scanning for viruses
- Identifying inappropriate use of systems
- Management of systems and networks (capacity, bandwidth and so on)
- Confirm compliance to policy

Reports on various activities may be generated and provided to management for action.

Inappropriate Content

Clients utilising the internet, who discover they have connected to any inappropriate website that contains sexually explicit, racist, violent or other potentially offensive material must immediately disconnect from that site. The ability to connect with a specific website does not imply that it is permitted to visit that site.

Unlawful Use

Clients must at all times comply with the state and federal laws and policies related to use of communication devices. Using SOPA's internet to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature is prohibited. Clients who do so may find themselves subject to criminal proceedings.

Clients must not engage in any use that may be considered questionable, controversial, offensive, obscene or could potentially damage the reputation of SOPA or the NSW Government.

Electronic Transactions

Clients engaging in personal electronic transactions via the internet do so at their own expense and risk. Any purchases or financial transactions conducted using SOPA equipment are done at their own risk.

Clients are reminded that details such as credit card numbers and passwords may be intercepted on the internet or within the SOPA environment as part of regular monitoring of electronic communications.

Downloads

Clients must take reasonable care when downloading from the internet to avoid unlawful and inappropriate access.

Security

Potentially, the supplied network could be used by unauthorised users connected to external systems. The client will take reasonable steps to ensure that unauthorised access to SOPA through their systems is not possible.

All equipment where applicable must have an up-to-date anti-virus software installed and must be scanned prior to connecting to the SOPA network. This equipment must be free from virus, Trojans, worms, spyware, key logging, sniffing, scanning software and any other software that may be used to bypass security controls utilised by SOPA.

Related Policies

Privacy Management Plan – POL 09/5

Contact Officer

Daniel Emerson
Timing, Scoring and Results Manager
Sydney Olympic Park Sports Venues
Phone: (02) 9752 3666
Mobile: 0427651518