**SCHWARTZ IT E-MAIL & INTERNET USAGE POLICY**
**GENERAL OVERVIEW**

**The Facilities**
Email, internet, telecommunication, closed circuit monitoring (CCTV), and most computer systems are handled by “Schwartz IT”, which is the IT arm of Schwartz Family Co. (SFC).

This covers all hotels, managed or non-managed, Sydney Brewery and related entities, Blue Sky Airways and other transportation modalities, Schwartz Family Co. administration offices, Matraville Medical Complex and related entities, and all other activities under the umbrella of Schwartz Family Co., Winadell Laudet P/L, Laudet P/L and Aldprop P/L and Straight 8 P/L.

 This policy is available on the www.sfc.org.au/policy website and it is a condition of employment or contracture, where any IT facilities are utilized, that this policy is adhered to. These facilities to allow them to communicate effectively with each other, and with the outside world, and to use the information gathering and storage capabilities that the facilities provide.

**Purpose**
The purpose of this policy is to preserve the integrity of the facilities by providing Guidelines for all users to clarify what constitutes appropriate conduct and usage of the facilities. These Guidelines are based on:

(a) Guidelines released on 30 March 2000 by the Privacy Commissioner’s Office which is part of the Federal Human Rights and Equal Opportunity Commission found at [http:\\www.privacy.gov.au/private/index.html](https://web.archive.org/web/20140629042752/http%3A/www.cafesydney.net/www.privacy.gov.au/private/index.html); and

(b) Guidelines released by the Human Rights and Equal Opportunity Commission concerning anti-discrimination and harassment found at [http:\\www.hreoc.gov.au/employerspage/policies](https://web.archive.org/web/20140629042752/http%3A/www.cafesydney.net/www.hreoc.gov.au/employerspage/policies).

**Compliance with Directions**
All users of the facilities must read this policy carefully and observe its requirements.
Compliance with this policy, including future amendments, is a condition of employment with any facility which uses Schwartz IT management. Any breach of any part of this policy will be regarded as a serious breach of employment and contractual obligations. Failure to comply with directions given by your department head and Information Technology Department or his/her designate can result in the following action:
• disciplinary action by your department head or his/her designate regarding “inappropriate use” of the facilities; “inappropriate use” of the facilities is not limited to unlawful conduct and will occur whenever your department head or his/her designate is of the opinion that a user has used facilities contrary to the operations or objectives of the relevant division or department;
• cancellation of access to any or all of the facilities; or
• dismissal from employment.

**How Can a User Contravene this Policy?**
The Schwartz Family Co. group of companies and the directors may be both directly and vicariously liable for the inappropriate or unlawful actions of users. Vicarious liability arises when an employer is liable for the action(s) of employees which are committed within the course or scope of their employment. In most cases, employers can only escape liability if they can show that they took all reasonable steps to prevent the actions in question from occurring.

An employer may also be directly liable under Federal and State legislation for unlawful use of Schwartz IT facilities including hut not limited to:
(i) New South Wales Anti-Discrimination Act 1977;
(ii) Federal Sex Discrimination Act 1994;
(iii) Federal Disability Discrimination Act 1992;
(iv) Federal Racial Discrimination Act 1975;
(v) Federal Crimes Act 1900;
(vi) Federal Copyright Act 1968; and
(vii) Federal Defamation Act 1974.

**Unacceptable Use**
Schwartz IT users must not use the facilities to:
• engage in any activity which is likely to be considered unlawful under the legislation referred to above or inappropriate in the opinion of your department head or his/her designate;
• annoy, interfere with or disrupt the reasonable use of the SFC network by any other person; and
• gain unauthorised access to information or other computer networks.

**Access, Storage and Distribution of Offensive Material**
Users must not draft, look up or distribute any material (including e-mails, screensavers and internet sites) which may be offensive to other persons.
(“Offensive Material” includes but is not limited to comments, opinions, jokes, pictures, or executable files that may be of sexual, racist or otherwise discriminatory effect.)
Users must not attempt to access information, data, or source code which is not necessary in their day-to-day activity.
Users cannot apply to storage, either by printing, or electronically, or electronic transmission, such information for purposes other than work related.

**Defamation**
Defamation occurs when a statement or publication injures the reputation of another person. Defamation can be a civil action or a criminal offence under relevant legislation. A user may be sued for defamation. Users are forbidden from distributing potentially defamatory comments by e-mail, mailing lists and notice boards.

**Copyright**
Copyright protects the exclusive right of the copyright holder to copy, publish, perform, broadcast and sell copyrighted material.
Users must respect the copyright and any other intellectual property rights of third parties. A user cannot download material from the internet or otherwise receive and use information that is owned by a third party unless they have the written permission of that party.
As a general rule, downloading from the internet for personal research is allowed but downloading material for distribution to others or for business use will require the permission of the third party owner.
Schwartz IT hosts many websites.

**Workplace and Sexual Harassment**
Computer and internet usage has created a new avenue for harassment including sexual, racial and other forms of harassment in the workplace.
Examples of facilities related harassment include the transmission of offensive, insulting and harassing e-mail messages, offensive screensavers or the accessing of sexually explicit websites through work computers.
Examples of unlawful sexual harassment include:
(i)when an employee makes personally offensive comments via e-mail;
(ii)when an employee uses the e-mail facility to tease a person, or make repeated comments about alleged sexual activities or their private life; and
(iii)when an employee uses the e-mail facility to make persistent or unwelcome social invitations.

**E-MAIL USAGE**

**(a) General**
Users of e-mail should:
(i) only use e-mail for ‘business purposes” which relate to Schwartz IT and the direct nature of Schwartz IT business;
(ii) ensure that attachments greater than 5MB are “zipped” using approved licensed compression software, or preferably sent by FTP (for details of this, ask our systems administrator);
(iii) delete attachments and e-mails from unknown origins without opening them to view their contents (most probably spam);
(iv) virus check any attachments from outside Schwartz IT prior to opening and advise the Executive Assistant Manager of any documents found to contain viruses. The person sending the infected file, should also be requested to install or update their virus checking software to prevent further contamination.
(v) refrain from using e-mail as a filing system. Any messages that need to be kept should be saved to a network directory, the appropriate location on the intranet or printed. All old e-mail messages will be deleted regularly by the Systems Manager. When your mailbox is nearly full, you will be warned, and then you will need to delete old mail
(vi) respond to any system support request to reduce the size of e-mail files in a responsible manner. Microsoft Outlook and Lotus Domino has a self-quota system that is imposed by the administrator. If the mailbox is full, and no attempt is made to reduce the size of the files, then you will get no more mail
(viii) pass onto the IT systems manager any unsolicited or offensive emails, or unusual virus alerts you receive and are unsure of.

**(b) Content**
Users should exercise good judgment and common sense when creating and distributing e-mail messages. Schwartz IT and/or individual users may be liable for any defamatory or misleading or deceptive statements contained in e-mail messages.
Users should check addresses and spelling carefully prior to sending any e-mail correspondence.
Users should make every effort to ensure that people from whom they expect to receive email are aware of the correct spelling of their address.

**(c) Signature**
E-mail messages sent to external parties may have a signature automatically appended by the e-mail system, but these serve no purpose from a legal standpoint.

**(d) Attachments**
Care must be taken when opening attachments, in case they harbour malicious viruses or malwear. In general, if an email is received from an unknown person, or one is received from a known contact that looks suspiciously different, it should NOT have attachments opened. There is nothing lost by replying to the person to confirm the validity of the email, prior to opening any attachment.

**(e) Schwartz Family Co. Property**
E-mail is made available to users to enable Schwartz Family Co. to conduct its business communications efficiently. All e-mail sent or received from Schwartz IT systems are the property of Schwartz IT.
Users should not expect that e-mail is confidential or private.
Schwartz IT retains the right to access or view users e-mail. System administrators have the right to access individual mailboxes of emails sent and received by the corporate network.
Schwartz IT does not log the content of e-mails, however, these e-mails may still be stored on mail servers. The Systems Administrator or his designate may access user e-mails and browse logs when alerted to abnormalities to mail traffic patterns, or if system logs suggest inappropriate activities have taken place.

**(f) Personal Use**
Schwartz IT acknowledges that e-mail may on occasion be used for “personal use” but reserves the right to limit such use. If an e-mail is personal, the user should make it clear that the message is not being sent on behalf of Schwartz IT. In such a case any personal company signature should be deleted.

**(g) Prohibited Use**
E-mail (including personal e-mail) cannot be used to:
(i) send e-mail messages (with or without attachments) which contain inappropriate material” which includes offensive material as defined above as well as any material considered inappropriate or unlawful as defined above;
(ii) distribute electronic chain letters, for example pyramid selling schemes of advertising;
(iii) send unauthorised e-mail from another users e-mail address or impersonating another user;
(iv) send e-mails which are likely to be perceived as harassment, intimidation or an unwanted invasion of privacy. Harassment includes circumstances in which a reasonable person in such circumstances would be offended, humiliated or intimidated:
(v) send non-urgent or non-work related e-mails to large numbers of users (whether within a SFC entity or not) at any time; and
(vi) send personal e-mail to any person who does not wish to receive it. If a recipient asks a user to stop sending him or her e-mail, the request must be observed.

**(h) Receipt of Offensive E-mail, other than automatically generated spam:** If a user receives offensive e-mail from outside Schwartz IT by e-mail, the user should immediately delete it and should not reply to the e-mail. The user may wish to forward the email to the Administrator for further action.

**(i) Discovery**
Users should be aware that e-mail communications may be discoverable in any legal proceedings in the same way as any other communication. This means that Schwartz IT may be required to disclose any e-mail communication that is relevant to any particular litigation to other parties.

**(j) E-mail Etiquette**
E-mail messages sent outside Schwartz IT should observe the same conventions as any other correspondence. All emails should be given appropriate titles. Users should use appropriate language and check e-mails for typographical and spelling errors before they are sent. Where the message would be longer than two or three screens, the documents should be sent as an attachment with a covering note.

**SOCIAL MEDIA USAGE**

1. **General.** Social media has helped to make the boundary between work and private less distinct. The reach of social media is often not anticipated, this in fact makes it an important use in marketing.

**(b) Content on SFC social media channels**
Users should exercise good judgment and common sense when creating and distributing any comments on social media.. Schwartz IT and/or individual users may be liable for any defamatory or misleading or deceptive statements contained in social media messaging.

**(c) Content on private social media channels**
All staff need to be aware that private comments can be transmitted over a wide social platform. Consequently, they should be aware of maintaining confidentiality of business information, as well as not giving cause for defamation accusations from staff and friends of clients (hotel guests) or staff that may have access to these private comments.

**INTERNET USAGE**

**Data Collection**
Schwartz IT may use social networking sites to collect data relevant to the role of a private IP (internet provider) which empolys personnel, taking into account the employees roles, and demographics of these employees.

**Business Use**
The internet can only be used between business hours for “work related purposes”.
“Work related purposes” is defined as any matter related to the nature of your work as stated in your Job Description.
Users may seek permission from their managers who access the internet for immoderate amount of personal use outside of business hours.
Schwartz IT reserves the right to charge users for personal use of the internet and to limit the rights of access to individual users.

**Access to Sites**
Users should be aware that internet sites accessed by users can record the IP address of Schwartz IT. Schwartz IT can monitor sites that users are accessing and it reserves the right to do so. Schwartz IT’s system administrators can monitor the date and time that websites were visited and the duration of site visits can be logged.
Users should therefore exercise discretion and only access sites relevant to the business of Schwartz IT.
Schwartz IT reserves the right to cancel user privileges or block access to sites which it deems to be inappropriate.
Schwartz IT reserves the right to publish figures which disclose how often a user has been using the internet to their manager or to those administering the system or managing the administrators.
Warning: A user who elects to access inappropriate or offensive material may be dismissed from his or her employment.

**Vending Information**
The internet is not a secure method of sending information. Therefore, when sending confidential information (for example business information, customer details, pricing, or any personal or private information about individuals), careful consideration should be given as to whether alternative means of communication are preferable.

**FACILITIES USAGE POLICY — COMPUTER SOFTWARE, HARDWARE AND THE SCHWARTZ IT NETWORK**
**Hardware**: Users are given or have access to appropriate computer equipment to carry out their job responsibilities. Such equipment will at all times remain the property of the workplace. Any equipment must not be removed from the users normal work area unless authorised by the Information Technology Department or his/her designate. Laptops should be safely stored at the workplace, unless otherwise specified.

**Passwords:** Employees shall not use a code unless authorised to do so. All computer pass codes (except for individual workstations) must be provided, on request, to the Administrator. Passwords should not be given to anyone else other than the designated Administrator on request. No other pass code may be used that is unknown to the company. Users should ensure that; they are logged off the network whenever leaving a workstation unattended; should not attempt to gain access to another user’s messages without permission; and users may be held responsible for any unauthorised access of the Schwartz IT network. Schwartz IT reserves and they exercise the right to restore a user’s password to a default value if access to user’s files or workstation is required by an authorised person in their absence.

**Software:** The use of any unauthorised unlicensed and/or illegal software is strictly prohibited. Any information system leased by or under contract to Schwartz IT should be treated as an information system owned by Schwartz IT with respect to security considerations.
User software is subject to the terms and conditions of the relevant copyright or license agreement of the product. Unauthorised copying of software is prohibited.
Users are forbidden from making additional copies for concurrent use on additional computers unless explicitly permitted by the license.
Users cannot create backup copies in support of the original unless this is explicitly permitted by the license.

**Floppy Disks, CD ROMs and memory sticks:**
Disks containing software from outside of Schwartz IT must not be used on workstations (ie. games, outside programs) unless authorised by the Information Technology Department or his designate and your supervisor.
Any internal disks or external drives connected by way of USB drives, from which information is required or any program must be scanned before copying or reading any files.
All external computer programs or documents must be virus checked prior to being installed or opened.
All workstations are equipped with anti-virus software. Such software should be used on a regular basis to ensure that viruses do not destroy vital information.
Any user who breaches this guideline by unloading files, which contain a virus, may be responsible for expenses to eradicate any damage.

Electronic Storage: Network or local hard drives should generally only be used to store work related material although a minimum of personal material is acceptable. The storage of inappropriate material is strictly prohibited. Individual file locations on a file server will be set up by the Systems Administrator and the method of access shown to you. This is preferable to storage of information on a local workstation hard disk which is not backed up.

**SFC WAN:**
Schwartz IT is interconnected by a wide area network. Unauthorised access on subnets beyond your own workplace is forbidden unless authorized by the IT department.

**FURTHER INFORMATION OR QUESTIONS:**
Please address them to jerry@schwartz.com.au