**Sheen Group Internet Usage Policy – 2025**

As an employee of Sheen Group using its information technology services, you are provided with access to the vast information resources of the Internet to help you do your job faster and smarter, and be a well-informed business citizen. The facilities to provide that access represent a considerable commitment of company resources for telecommunications, networking, software, storage, etc. This E-Mail and Internet Usage Policy is designed to help you understand our expectations for the use of those resources in the particular conditions of the Internet, and to help you use those resources wisely.

This policy applies to all users of Sheen Group owned and operated computer systems and networks. The word ‘company’ in the following text means Sheen Group or any organization using Sheen Group owned or managed systems. Any exceptions to this policy require the express written consent of the Sheen Group Management.

Any employees who discover a violation of this policy shall notify Sheen Group’s management immediately.

Any employee who violates this policy or uses the Internet system for improper purposes shall be subject to discipline.

**1.** The use of Sheen Group’s Internet and e-mail systems is intended for Sheen Group business including staff research, communication, and professional development within the broad business objectives of the company.

**2.** The company has software and systems in place that can monitor and record all Internet usage. Internet Activity may be review at any stage.

**3.** The confidentiality of any electronic message using Sheen Group’s e-mail or Internet system should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message.

**4.** Personal use of Internet and e-mail services cannot interfere with business operations and normally should be limited to non-working hours (breaks, lunch).

**5.** E-mail and Internet services, or any other network or computer resources, shall not be used for viewing, archiving, storage, distribution, editing or recording of threatening, obscene, harassing or derogatory material; or transmittal of material that is confidential to the company.

**6.** E-mail and Internet services, or any other network or computer resources, shall not be used for the viewing, archiving, storage, distribution, editing or recording of any kind of sexually explicit image, material or document.

**7.** Employees are reminded that social media platforms, Facebook and Twitter are public forums where it is inappropriate to reveal confidential company information, customer data, trade secrets, and any other material covered by existing company secrecy policies and procedures. Employees releasing protected information via a social media avenue – whether or not the release is inadvertent – will be subject to disciplinary procedures.

**8.** The social media (Facebook, twitter), chat rooms, newsgroups and e-mail of the Internet give each individual Internet user an immense and unprecedented reach to propagate company messages and tell our business story. Because of that power we must take special care to maintain the clarity, consistency and integrity of the company’s image and posture. Anything any employee writes on the Internet in the course of working for the company can be taken as representing the Sheen Group’s corporate posture. For this reason, users of Sheen Group’s e-mail system are prohibited from using their Sheen Group e-mail address (e.g. example@sheengroup.com.au) or otherwise identifying themselves as employees of Sheen Group when participating in non-work related online discussion forums, bulletin boards, web sites, or chat sessions.

**9.** Only those employees who are duly authorized to speak to the media/social media or in public gatherings on behalf of the company may speak/write in the name of the company to any newsgroup or chat room. Other employees may participate in newsgroups or chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves. Where an individual participant is identified as an employee or agent of this company, the employee must refrain from any unauthorized political advocacy and must refrain from the unauthorized endorsement or appearance of endorsement by the company of any commercial product or service not sold or serviced by this company, its subsidiaries or its affiliates. Only those managers and company officials who are authorized to speak to the media, to analysts or in public gatherings on behalf of the company may grant such authority to newsgroup or chat room participants.

**10.** Sheen Group has no control over the information or content accessed through the Internet and cannot be held responsible for its content.

**11.** Use of the e-mail or Internet systems to receive (download) software programs, utilities or software extensions is prohibited without prior authorization from Sheen Group’s Network.

**12.** Any software or files downloaded via the Internet into the company network become the property of the company. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

**13.** No employee may use company facilities knowingly to download or distribute pirated software or data. The use of file swapping software on company computers and company networks is prohibited.

**14.** No employee may use the company’s Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

**15.** No employee may use the company’s Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

**16.** This company’s Internet facilities and computing resources shall not be used knowingly to violate the laws and regulations of Australia or any other nation, or the laws and regulations of any state or city. Use of any company resources for illegal activity is grounds for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.

**17.** Users of Sheen Group’s information systems are prohibited from using password protection to restrict access to files on Sheen Group systems, without authorization from Sheen Group’s Network Administrator.

**18.** Each employee using the Internet facilities of the company shall identify himself or herself honestly, accurately and completely (including one’s company affiliation and function where requested) when participating in chats, newsgroups, Facebook posts or when setting up accounts on outside computer systems.

**19.** The company retains the copyright to any material posted to any forum, social media platform or World Wide Web page by any employee in the course of his or her duties.

**20.** Use of company Internet access facilities to commit infractions such as misuse of company assets or resources, sexual harassment, unauthorized public speaking and misappropriation or theft of intellectual property are also prohibited by general company policy, and will be addressed under the relevant provisions of the Employee Handbook.

**Sheen Group Intranet**

I understand and agree that the information/data I have been authorised to access is considered highly confidential. Under no circumstances will such information be used by me, conveyed or discussed with a third party unless required in the course of my duties. Failure to abide by these access rules may result in legal action against the individual.

Sheen Group’s Network Administrator: James Black 9427 1666, mobile 0437 089 005 email james.black@sheengroup.com.au

**DATE:**

Employee:

Employee Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Manager Name:

Manager Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_