1 Liddall Way,
Horton Road
West Drayton,
Middlesex, UB7 8PG
Tel: 01895 432 995
Fax: 01895 432 976
simon@systemsound.com

I.T. Policy Statement

Computers, networks and electronic information systems are essential resources in the day to day running of System Sound & Light Ltd. The Company allows all members of staff access to e-mail and the World Wide Web if used in a responsible and effective manner.
Users must be aware of their right and responsibilities, which outline liability for personal communication, privacy and security issues, and consequences of violations.

The Company has an obligation to abide by all relevant legislation. This policy and supporting policies, procedures, guidelines and standards must satisfy all applicable legislation. This obligation formally devolves to all users of computers at work, who may be held personally liable for any breach of the legislation.

If anyone finds an inconsistency between policies and legislation, or between individual policies, they must bring this to the attention of the one of the partners.

I.T. Policy

1. Users must comply with current British legislation in all respects when using IT systems and equipment. Legislation, which applies particularly to these circumstances, is:

i. The Health and Safety at Work etc. Act and the work of the Health and Safety Executive.
ii. The Computer Misuse Act 1990.
iii. The Data Protection Act 1998.
iv. The Data Protection Registrar.
v. The Regulation of Investigatory Powers Act 2000.
vi. The Communications Act 2003.
vii. The Copyright, Designs and Patents Act 1988.
viii. The Copyright Licensing Agency.

2. No user may copy programs or information to paper, removable media (such as floppy disks), non-removable media (such as hard discs) or to portable computers except where explicitly allowed by the license agreement/contract and where no copyright or intellectual property right is infringed.

3. No user may interfere with protection systems. This includes: any device which is provided to prevent removal or theft of equipment; any software or configuration that detects or prevents virus infection; any software or configuration that prevents the running of non-approved software.

4. No user may install or use software or systems that are not licensed for use.

5. Company computers may not be used to transmit, store or access text, images, recordings, scripts, programs or telephone calls that contain:

    i. Material likely to contravene current legislation or cause upset to other employees, such as sexist, racist, homophobic, xenophobic, pornographic, paedophilic or discriminatory material.
    ii. Text, images or recordings to which a third party hold copyright or other intellectual property right, without the written permission of the right-holder.
    iii. Material that is defamatory, libelous, slanderous or threatening.
    iv. Material that could be used to breach computer security or to facilitate unauthorized entry into computer systems.
    v. Material that is likely to prejudice or seriously impede the course of justice in UK criminal or civil proceedings.
    vi. Material containing personal data as defined by the Data Protection Act 1998 unless the subjects' permission has been explicitly given in writing.

6. The Company may intercept any communication transmitted across or stored on its systems provided that this is within the framework of the RIP Act 2000. In particular, it may monitor but not record communications.

    i. To anonymous help lines
    ii. To determine whether communications are for personal or business purposes

7. The Company may monitor and record communications for the following purposes:

    i. To ensure that users are complying with Company policies, Conditions of Use, procedures and guidelines and with British legislation, except that recording may not take place the criteria in item 6.
    ii. To monitor standards of quality, performance and security.
    iii. To prevent or detect crime.
    iv. To investigate unauthorized use of systems.
    v. When an external agency requests information under the RIP Act, the IT Manager will be the point of contact. In his absence, the Office Manager shall be the point of contact.
    vi. The Company randomly logs transactions on its systems. This logging covers the transmission of e-mails, access to Web pages and logging in and out of user network accounts.

NOTE:

Company e-mail systems and Web access are provided for the conduct of company related business. Incidental and personal use of these systems is permitted so long as such use does not disrupt or distract the individual from Company business (due to volume, frequency or time expended) and that it does not incur unreasonable cost to the Company, and/or does not restrict the use of those systems to other legitimate users.
Users are reminded that the Company can access their e-mail messages for operational and security purposes.