



For better
mental health

Sheffield Mind Ltd

Lawton Tonge House
57 Wostenholm Road
Sheffield S7 1LE

T: 0114 258 4489

F: 0114 250 0729

w: www.sheffieldmind.co.uk

e: office@sheffieldmind.co.uk

ICT Acceptable Use Policy

Purpose of this policy

The following policy has been produced in order to safeguard the interests of Sheffield Mind, its staff and volunteers. All Sheffield Mind's IT facilities and information resources remain the property of Sheffield Mind and not of particular individuals. By following this policy we'll help ensure IT facilities are used:

- legally;
- securely;
- without undermining Sheffield Mind;
- effectively;
- in a spirit of co-operation, trust and consideration for others; and
- that they remain available.

Disciplinary measures

Any contravention of this policy will be dealt with under the appropriate procedures. This may involve the disciplinary procedure being invoked. Since this policy refers to minor issues through to illegal activities, the sanctions for breaches may range from informal warning to summary dismissal.

General principles

The Internet (web and email) can be an extremely useful tool for the furtherance of Sheffield Mind's objectives. However, Internet browsing should be used in a responsible manner.

Legal considerations

- The Data Protection Act 1998 applies to email as it does to all forms of stored information. ICT users must be mindful of this and ensure that an email containing personal data:
 - is not disclosed to unauthorised persons; and
 - is only kept if it is required for work purposes, and
 - is kept secure (including printouts).

Only keep email which needs to be kept. Users are responsible for managing their own emails and ensuring they are kept secure. So, **keep your password safe.**

- Copyright: Take care to use software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and could result in criminal charges.
- The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you don't have access to information resources you feel you need, contact your supervisor.

Points for individuals to consider

1. Information of a proprietary confidential or sensitive nature must not be disseminated or disclosed outside of Sheffield Mind.



For better
mental health

2. You must not use any communication means (post, email or the Internet) for the creation or transmission of defamatory or libellous material.
3. Intellectual property rights must not be violated. Also permission must be sought from the copyright owner before sending or publishing copyrighted material.

NB. Users should report to their supervisor any suspected illegal or unauthorised use of Sheffield Mind's email services or Internet access.

Security

It is important to be security conscious and to adhere to Sheffield Mind's security procedures as set out in the Information and Communication Technology Policy. This can be viewed in the policies folder on the server.

Offensive material

Email and the Internet should not be used to view, create or transmit any offensive, obscene or indecent images, data or other material. Avoid sending anything that may be considered offensive, e.g. any racial, sexual or religious abuse, or an angry response email. Users who experience any offensive email should inform their supervisor, the CEO, a Director or the Office Manager. Any such offence by a member of staff, volunteer or director will be treated seriously.

Software received with email or downloaded from the Internet

Users who intend to receive software by email or to download software from the Internet, must first check with the Office Manager. Any download must comply with their software policies.

Privacy

Email cannot be considered private. Users should be aware that, on occasion, the Office Manager may, during the performance of his/her IT support duties, inadvertently see the contents of email messages or Internet activity. Also that the mere deletion of a message or file may not necessarily eliminate it from the system. Generally, consent of the author will be sought prior to any inspection, monitoring or disclosure of email records in the user's possession.

To meet business or service needs, or where legal issues are involved, management reserves the right to inspect such records without the user's consent.

Unacceptable use of the Internet

In particular the following is deemed unacceptable use or behaviour by employees:

- visiting Internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- using the computer to perpetrate any form of fraud, or software, film or music piracy
- using the Internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- hacking into unauthorised areas



For better
mental health

- publishing defamatory and/or knowingly false material about Sheffield Mind, your colleagues and/or our customers on social networking sites, "blogs" (online journals), "wikis" and any online publishing format
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of malicious software into the corporate network

Unacceptable use of email

- use of company communications systems to set up personal businesses or send chain letters
- forwarding of company confidential messages to external locations
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- accessing copyrighted information in a way that violates the copyright
- breaking into the company's or another organisation's system or unauthorised use of a password/mailbox
- broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- transmitting unsolicited commercial or advertising material
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of computer virus or malware into the corporate network