Internet, Email and Social Media Policy

Internet usage

Access to the Internet or other external systems is provided for charity purposes. Access may be granted for ‘Charity sponsored’ activities such as studying for recognised qualifications. In these cases, prior approval must be obtained from your line manager or a Trustee.

The Charity recognises that occasionally employees may wish to use the Internet for personal reasons. For security reasons personal use is not permitted.

Users must not access any Internet sites that contain obscene, extremist or other objectionable material, such as sites displaying sexual or pornographic images. Not only will this be deemed gross misconduct, but certain images such as paedophilia will also be reported to the police. If any site which could be construed as one described above is visited accidentally, then the incident must immediately be reported to your Line Manager. A failure to do so will result in disciplinary action being taken, which may result in dismissal.

Users must not use the Internet for gambling, conducting illegal activities or soliciting for personal profit.

Users must ensure that they do not permit others to misuse their PC. Therefore all PC’s that have access to the Internet should be password protected so that when the user is away from their desk the system cannot be misused. Employees must not disclose their passwords to a colleague unless given permission to do so by their line manager.

Email usage

Access to the Charity’s email facilities is provided by the Charity for business purposes. Access may be granted for ‘Charity sponsored’ activities such as studying for recognised qualifications. In these cases, prior approval must be obtained from the appropriate line manager.

The Charity recognises that occasionally employees may wish to use email for personal reasons. Personal use is permitted provided:

1. Use is occasional and it does not interfere with the employee’s work and the content of emails sent is appropriate to the workplace.

2. Users must not solicit internal or external emails that are unrelated to the Society’s business activities.

Users must not send any information emails from their work email account to their personal / home e mail accounts. If there is a need to send information in this way the information must be sent via an encrypted secure email.

Users must not send, internally or externally, or save on their systems, emails containing indecent, obscene or libellous material, material likely to cause offence or any material containing comments about individuals, which might be construed as offensive.

If an employee sends an email containing indecent, obscene, libellous or offensive material this will be treated as an act of gross misconduct and may result in summary dismissal.

If an employee receives an email containing indecent, obscene, libellous or offensive material they should immediately bring the matter to the attention of their line manager. Such emails must not be saved or forwarded to other users. Any breach of this rule will be treated as gross

misconduct and the rule will apply regardless of whether the email is sent/saved/forwarded during or outside of normal working hours.

It is an unfortunate fact that, just like normal junk mail, unsolicited email (referred to as ‘Spam’) is a problem. Examples include advertising, ‘get rich’ schemes and chain letters. There are a number of things that users can do to help mitigate the problem.

1. “Spammers” can harvest email addresses from postings made to newsgroups. Keep such postings to a minimum.

2. Do not give out your email address except to associates or customers.