Internet Usage Policy

Introduction

This is a corporate statement of good computer practices to protect Acuity Research and Practice Ltd from casual or intentional abuse. With the growth in use of e-mail and access to the Internet throughout the organisation, there are a number of threats and legal risks to the company, as well as the potential costs of time wasting, that can be avoided by following the practices outlined.

Although both these tools are provided first and foremost for business use, Acuity accepts that on occasion they may be used for personal use. At all times users should take into account these guidelines and adhere to them.

These guidelines apply to all employees who have access to e-mail or the Internet.

Access

The Internet is a rich information resource and is provided by Acuity to enhance the work, learning and personal development of our people. Access to the Internet is provided in different ways, and this policy is intended to govern all internet use that is provided by or paid for by Acuity.

The Internet is primarily provided to support business related activities - work, communications, research and career development. The facility may also be used for occasional and limited personal use.

All staff are responsible for ensuring that their Internet usage is within the regulations and is ethical and lawful. The downloading of text or images which contain material of an offensive, indecent or obscene nature is prohibited.

Acuity provides equipment and internet connections to members of staff to enable them to work from home. It is not desirable or practicable to prevent staff using the equipment or bandwidth for their own personal use. However, members of staff are responsible for ensuring that any personal usage does not interfere or impact upon the availability of the internet or equipment for business purposes.

E-mail

This policy should be read in conjunction with the Acuity email policy and guidelines, summarised here.

- Personal Use. Employees are permitted to send personal e-mails on a limited basis as long as this does not interfere with their job responsibilities. It should be noted that any e-mail messages are not guaranteed to be private and remain the property of Acuity.
- Confidentiality. Messages sent and received via the Internet are regarded by the Company's Act as having the same legal status as a corporate letter. Any material that is viewed as highly confidential or valuable to the Department should not be e-mailed externally.
- A disclaimer document will be attached to all e-mails with an individual signature for each user. In no instance should the disclaimer be tampered with, although if necessary the signature can be altered.
- It should be remembered that the Internet does not guarantee delivery or confidentiality.
- It should be noted that there are systems in place that can monitor, review and record all e-mail usage, and these will be used. Analysis of this information may be issued to managers if thought appropriate. No user should have any expectation of privacy as to their e-mail.
- Etiquette. At all times users should use appropriate etiquette when writing e-mails, e.g. e-mails should not be written in capitals as this can be perceived as 'shouting'. Guidance on "netiquette" can be provided if requested. These include warnings about the need to be careful about addressing e-mails, particularly when using address groups, in order to send them to only those recipients who will have an interest.
  In some instances, where the nature of a message may be deemed confidential, it may be appropriate to notify, or even seek permission from, the original sender before forwarding a message onto another recipient.
- Dissemination of Information. In cases where information of a general nature is circulated via e-mail of on an electronic notice board, database or web site, it is the responsibility of the relevant manager or supervisor to ensure that members of their staff who do not have access to the system are notified of the information
- Inappropriate behaviour. Users should not send messages that contain any unsuitable material or defamatory statements about other individuals or organisations.
  Messages should not contain material or language that could be viewed as offensive to others or as contravening the Acuity Equal Opportunities Policy, N.B. what may appear appropriate to one person might be misconstrued by another.

- Material, which could be construed as canvassing, lobbying, advocacy or endorsement should not be sent by e-mail.

If in doubt, consult a Director

- Virus Protection. To prevent the risk of potential viruses, users should not open any unsolicited e-mail attachments or independently load any software, including screensavers, onto their computers. If a user does inadvertently open a message or attachment that contains a virus, they should immediately close the message and attachment. It should not be accessed again without approval from IT.
- In some instances, it might be appropriate to inform the original sender that their message contained a virus.
- Email is an effective way of communicating confidential information. This is only the case, however, if passwords are secure. It is good practice for users to change their passwords regularly.
  Email should not be left running unattended in any circumstances where this may lead to unauthorised access. The system should be closed and re-opened on return. In no instances should a user login using a colleague's password unless permission has been given.
- Where access to a mailbox is required. Prior permission must be received from the individual concerned or their line manager/Director.
- Good housekeeping practices should be adopted so that files are deleted regularly or, if necessary, archived to a separate file. Mailbox sizes will be reviewed regularly and warnings will be issued to users where appropriate regarding files stored. File attachments, incoming or outgoing through the firewall, are limited to 15MB but good practice is that file attachments should only be sent to a minimum of recipients and not all if they are large files.

Responsibilities of Internet Users

Users of the Internet must adhere to the following:

1) Users must never attempt to transmit, or cause to be transmitted any message in which the origin is deliberately misleading;
2) If a user does transmit, or cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origin, the person who performed the transmission will be solely accountable for the message and not Acuity which is solely acting as the information carrier;

3) Any user who finds a possible security lapse on any system is obliged to report the event to a Director;

4) Users must not, without prior approval from a Director utilise any of the following technologies: routing, forwarding. Bridging, ARP proxying, IP masquerading, Network Address Translation (NAT), IP/IPX tunnelling, SOCKS, application layer proxies, SSH, and peer-to-peer (P2P) on any computer connected for the purposes of sending data to or receiving data from an externally located machine.

Downloading

- Any software or files downloaded via the Internet onto Acuity equipment may be used only in ways that are consistent with their licences or copyrights.
- No user may use Acuity facilities knowingly to download or distribute illegal software or material.
- No user may use Acuity Internet facilities to propagate deliberately any virus.

Chat, social media and newsgroups

- Chat and social media such as MS Teams may be used but solely for business purposes. Other purposes of chat and messaging are prohibited. Chat, social media and newsgroups are public forums and confidential company or personal information must not be revealed.
- Users of any chat Internet facilities must identify themselves honestly, accurately and completely when participating in chats or newsgroups.
- Users may participate in newsgroups or chats in the course of their work or research, but they do so as individuals, speaking only for themselves. Only those users who are duly authorised to speak to the media on behalf of Acuity may write in the name of the company to any newsgroup or Web site.
- Acuity retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any employee in the course of their duties.

Social Media

The Company does not object to you setting up personal accounts on social networking websites or blogs on the internet, in your own time and using your own computer systems. However, you must not do so on Company media or in work time.

You must not link your personal social networking accounts or blogs to the Company's website. Any such links require the prior consent of a Director.

You must not disclose Company secrets, breach copyright, defame the Company or its clients, suppliers, customers or employees, or disclose personal data or information about any individual that could breach the Data Protection Act 1998 or GDPR on your blog or on your social networking website.

Social networking website posts or blogs should not be insulting or abusive to employees, suppliers, Company contacts, clients or customers.

References to the Company

If reference is made to your employment or to the Company, you should state to the reader that the views that you express are your views only and that they do not reflect the views of the Company. You should include a notice such as the following:

'*The views expressed on this website/blog are mine alone and do not reflect the views of my employer*'

You should always be conscious of your duty as an employee to act in good faith and in the best interests of the Company under UK law. The Company will not tolerate criticisms posted in messages in the public domain or on blogs about the Company or any other person connected to the Company.

You must not bring the Company into disrepute through the content of your website entries or your blogs.

Any misuse of social networking websites or blogs as mentioned above may be regarded as a disciplinary offence and may result in dismissal without notice.

You should be aware that any information contained in social networking websites may be used in evidence, if relevant, to any disciplinary proceedings.

Auditing

- Under the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Acuity reserves the right to monitor and record Internet usage patterns. Acuity can monitor and record all Internet usage. ICT does not routinely inspect Internet usage but may inspect any or all files that are stored on Acuity resources to the extent necessary to ensure a compliance with Acuity policies. Acuity reserves the right to do this at any time. Such inspection of files requires the authorisation of a Director. Users should not have any expectation of privacy as to their Internet usage.

- If Acuity is apprised of third party defamatory content on company servers, then Acuity will follow its procedures and will take all reasonable steps to remove or deny access to it.

Misuse of the Internet

- Action will be taken under the Acuity Disciplinary Policy against any users who are found to breach the policies outlined in these guidelines. Significant abuse, particularly involving access to pornographic or offensive or images constitute gross misconduct leading to summary dismissal.

Review

It is the responsibility of the Directors to review regularly the content of the Internet Usage policy.

Version: Internet Usage Policy v2023.Docx
Last Reviewed: 14 December 2022
Next Review: 31 December 2023