Acuity Email Policy & Guidelines for use

Introduction

Email is an important method of communication and the purpose of this policy is to describe the acceptable use of Acuity email and related services, systems and facilities.

Scope of the Policy

1. This Policy applies to all Acuity staff and any other authorised users. It covers the use, for the purpose of sending or receiving email messages and attachments, of any IT facilities provided by Acuity, including hardware, software and networks.
2. The Policy describes Acuity position on:
    - The personal use of email
    - Potential monitoring or interception of email
    - Third party access to email

Responsibilities

1. Responsibility for developing and updating this policy lies with Acuity acting, if appropriate, on the advice of the Director responsible for ITC.
2. All users, whether they create or receive emails, have a responsibility to ensure they make appropriate and proper use of the system, and that they comply with this policy and the guidelines provided by Acuity. See Appendix B.
3. Any member of staff who fails to comply with the Policy and the guidelines may be subject to disciplinary action. It is the responsibility of Directors to ensure that all staff are made aware of the existence and content of the Policy and of the guidelines.
4. Staff found to be in breach of this Policy and the guidelines may be subject to disciplinary action.
5. Any other authorised user who breaches the policy may have any privileges in relation to appropriate Acuity facilities withdrawn.

Third party access to email

1. In cases of absence Acuity may provide access to an employee's email account for business purposes. This type of access must be approved by a Director. The request, the reasons behind it, the extent and duration of access, and action taken will be logged.

2. Once approval has been given, the email administrator will arrange access in accordance with instructions from the Director. When it is appropriate, the owner of the email account should be advised of what has happened.
3. It is important, in this process, that any emails which are clearly private or personal are treated as confidential.

Personal Use

1. Acuity provides a range of computing facilities and resources for authorised users pursuing legitimate Acuity interests. While users may have the use of an email address(es) while they are authorised users, Acuity retains ownership of that address and all other parts of the email facility.
2. Acuity accepts, however, that appropriate use of e-mail for private non-commercial purposes is permissible. This use should, nevertheless, not require Acuity to provide additional resources over that which it provides for business use.
3. Users should ensure that emails addressed to or sent by them for private purposes are marked as personal, in order to distinguish between business and private emails.
4. Users should, however, be aware that the privacy of emails cannot be guaranteed, messages can be intercepted or wrongly addressed and they are easily forwarded to third parties.
5. Users must adhere to Acuity guidelines in Appendix B when using the system for personal purposes.

Personal use by staff

1. Personal use of the email system may take place in an employee's own time provided it does not interfere with the smooth running of Acuity, or deny resources to other users.

Appendix A

Definition of terms

Email systems

This covers any IT facilities provided by Acuity, including hardware, software and networks, for the purpose of sending or receiving email messages and attachments.

Users

This covers:

1. All staff using the email systems
2. Any other authorised individual using the email systems

Appendix B

Guidelines on email use – to be read in conjunction with Acuity email policy

1 Introduction

A written email policy and guidelines, known to all staff, establishes the boundaries and uses that may be made of Acuity equipment and infrastructure. Adhering to this guideline document will:

1. facilitate implementation of the Acuity email policy
2. help users avoid legal risks that they might inadvertently take
3. notify users of any privacy expectations in their communications
4. prevent damage to systems
5. avoid or reduce inappropriate time being spent on non-work-related activities
6. help protect Acuity against liability for the actions of its staff.

2 Legislation

All users of Acuity email system must comply with the relevant legislation.

Users should remember that the laws of the land relating to written communication apply equally to email, including laws on data protection, freedom of information, defamation, copyright, obscenity, fraud and wrongful discrimination.

An employer is vicariously liable for negligent acts or omissions by their employee in the course of employment whether or not such act or omission was specifically authorised by the employer. To avoid vicarious liability, an employer must demonstrate either that the employee was not negligent in that the employee was reasonably careful or that the employee was acting in their own right rather than on the employer's business.

3 Personal Use

The email system is provided to facilitate the work of Acuity. This applies to both staff and associates.

Acuity accepts, however, that using email for private non-commercial purposes is permissible, provided it does not interfere with the smooth running of Acuity, or deny resources to other users. Staff or associates should ensure that they do not make inappropriate use of the system.

4 Inappropriate use

Inappropriate use includes, but is not limited to, the creation or transmission of emails:

1. that bring Acuity into disrepute
2. that consist of unsolicited commercial or advertising material, chain letters or other junk-mail of any kind
3. that infringe the copyright of another person, including intellectual property rights
4. that unreasonably waste staff effort or networked resources, or that unreasonably serve to deny service to other users
5. that contain any offensive, obscene or indecent images, data or other material
6. that are designed to cause annoyance, inconvenience or anxiety to anyone
7. that include material which is sexist, racist, homophobic, xenophobic pornographic, paedophilic or similarly discriminatory and/or offensive
8. that contain defamatory material
9. that contain material that includes claims of a deceptive nature
10. that by intent or otherwise harass the recipient
11. that violate the privacy of others, or unfairly criticise or misrepresent others
12. that are anonymous messages or deliberately forged messages or that have deceptive email header information (ie without clear identification of the sender).

5 How to use email appropriately

Receiving email

1. Check your email regularly. Monitoring your emails should not be onerous, but regular monitoring of them is essential
2. All staff are expected to check their email every two hours or at key points of the day
3. Staff covering support email addresses are expected to check emails every two hours or at key points of the day or as agreed
4. Staff to apply the same courtesy to internal and external emails
5. Business out of office messages should always be set if you are away for half-a-day or more. Your out of office message to be professional and have the details of who to

contact if the matter cannot wait, the office number (if different) and the Acuity info email address.

Sending email

1. Always remember that sending email from your Acuity account is equivalent to sending a letter on Acuity letterhead.
2. Make sure that you use the 'subject' line in every message, and that it is meaningful. Where someone receives many messages, it helps to be able to judge the subject matter correctly from its subject line.
3. Try to restrict yourself to one subject per message, sending multiple messages if you have multiple subjects. This helps recipients to use the 'subject' line to manage the messages they have received.
4. Create a 'signature' and use it. Most email programs allow you to create a few lines of text that appear at the end of every email. You can use your signature to provide information such as your role and telephone number.
5. Try to keep email messages fairly brief.

Delete unwanted messages to conserve disk space.

Develop an orderly filing system for those email messages you wish to keep and delete any unwanted messages.

Replying to email

1. Reply promptly, expectation for Staff to respond to an email within 2 hours where possible (including emails received in support email addresses).
2. If Staff are not able to respond to an email straightaway or if additional work is required, they should reply to the sender within 2 hours where possible to acknowledge the email and to inform them when they will be able to respond fully
3. As a minimum adhere to Acuity's Customer Service Standards policy which outlines acknowledgement of all email enquiries within one working day, sending an initial response within three working days. A full reply to be given within 10 working days
4. When you use the 'reply' option, ensure that the subject field (automatically filled in for you) still accurately reflects the content of your message.
5. Be careful when using 'cc' and 'bcc'. Only copy the email to those people who really need to see it.
6. When replying include a relevant chunk of the original message – replying to a message with just 'I don't think so' can be confusing even with a relevant subject line

Forwarding email

1. Think twice before forwarding to someone else an email you have received. Would the author expect or be willing for this to happen?
2. The laws of copyright must be respected. It is not, in general, legal to forward material without permission from the copyright owner.

Good manners

1. Be careful how you express yourself. Email can easily convey the wrong impression.
2. Remember that people other than the person to whom it's addressed may see your message.
3. Never email something you wouldn't say to the recipient's face.
4. Don't criticise other people harshly. Assume that the email will be forwarded to them and will be read by them.
5. Don’t forward email to other people without informing the author.
6. Don't send unnecessary attachments. If you must send an attachment, give the recipient advance warning

Storing email

1. Delete all unwanted messages in order to conserve disk space.
2. Business critical information should be stored on the Acuity file system (MS Office 365 SharePoint system) which is secure and backed-up.
3. Develop an orderly filing system for those email messages you wish to keep.
4. Create a mail folder to store your personal messages.
5. Remember that stored messages are not password-protected – anyone with access to your computer will be able to read them

Legal Issues

1. Remember that any email you write or store may be liable to be disclosed under the Data Protection Act 1998, GDPR or the Freedom of Information Act 2002.
2. Don't make changes to someone else's message and pass it on without making it clear where you have made the changes. This would be misrepresentation.
3. Remember that the various laws of the land relating to written communication apply equally to email messages, including the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, and wrongful discrimination.

6 Confidentiality

1. Email is not secure. Do not put anything in an email message that you would not want read by everybody.

2. The commonest breach of confidentiality is wrongly addressed mail.
3. If you receive a message intended for someone else, let the sender know.
4. Anything you receive may not have originated from where it says it does, as email headers are easily forged. Therefore never disclose anything confidential, such as your password or credit card number, in an email message.
5. Be aware that the recipient of your message might forward it to others without recognizing the need to seek your consent. You cannot be sure who these other recipients will be

7 Interception of email

In general, the privacy of the content of emails will be respected.

There will be exceptional circumstances, however, when Acuity may require access to email accounts including their contents. These reasons include:

1. leave, where an employee or associate is not dealing with their email and this adversely affects the running of Acuity or a project.
2. to fulfil a legal requirement e.g. a Subject Access Request under the Data Protection Act.

Where the content of emails is to be accessed for either of the above purposes, the action must be approved by a Director and that action logged (see Acuity Email Policy Section IV).

8 Legal considerations

Human Rights Act 1998

This provides for the concept of privacy – giving a 'right to respect for private and family life, home and correspondence.' The provision is directly enforceable against public sector employers, and all courts must now interpret existing legislation in relation to the Human Rights Act.

Regulation of Investigatory Powers Act 2000

This Act covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system, and applies to public and private communication networks. It gives the sender or recipient of a communication the right of action for damages against the employer for the unlawful interception of communications.

Data Protection Act 1998

Individuals have a right, within certain limits, to have a copy of any personal data Acuity holds about them. Personal data includes any expression of opinion about an individual, whether held on paper or electronically. The individual's right of access may extend to material held in an individual's email mailboxes, or on the server.

Freedom of Information Act 2002

Acuity has only 20 working days to supply information requested under this Act. The Information Commissioner has made it clear that he will interpret the 20 working days as beginning the day after the request is made. In other words, an FoI request made by email will be deemed to have been received by Acuity without it even having been opened. The request may also cover material contained in emails in an individual's mailboxes.

Copyright law

The Copyright, Designs and Patents Act 1988 (as amended) gives the same protection to digital and electronic publications as it does to printed books and other forms of publication.

Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988 These acts are concerned with material that might be criminal, cause harm to young persons or be otherwise unlawful. Circulating text or images via email might subject an individual to charges of criminal behaviour.

Privacy and Electronic Communications (EC Directive) Regulations 2003

This covers unsolicited direct marketing activity by telephone, by fax, and by email.

Malicious Communications Act 1988

This act deals with the offence of sending letters etc with intent to cause distress or anxiety and states:

It is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person.

The Protection from Harassment Act 1997

This act was mainly passed in order to deal with problems in the law applying in England and Wales

GDPR

The **EU General Data Protection Regulation (GDPR)** effective from May 2018 gives all EU citizens more rights and protections for their personal data, to minimise the possibility of theft and fraud. Acuity continues to comply with GDPR even though the UK has left the EU. These regulations include provisions for the following areas:

- **The right to be informed**: Companies must publish a privacy notice, in addition to explaining transparently how they use this personal data.
- **The right of access:** Individuals will have the right to demand details of any of their data that a company may hold. This information must be provided within one month of request at no charge to the individual.
- **The right to rectification**: If a person's data is incorrect or incomplete, they have the right to have it corrected. If the company that holds the information has passed any of that information to third parties. The company must inform the third party of the correction and inform the person which third parties have their personal data.
- **The right to be forgotten**: A person may request the removal of their personal data in specific circumstances.
- **The right to restrict processing**: Under certain circumstances, an individual can block the processing of their personal data.
- **The right to data portability:** A person can access their data for their own use anywhere they prefer.
- **The right to object**: A person can object to the use of their personal data for most purposes.

Version: Email_Usage_Policy V2024.Docx

Last Reviewed: 28 December 2023

Next Review: 31 December 2024