Email acceptable use policy

Overview

This email acceptable use policy outlines the permissible use of business email for iQuda & email users at iQuda, when sending and receiving emails using an iQuda email account either in the workplace or remotely.

Purpose

The purpose of this policy is to ensure the proper use of email at iQuda, so that users are aware of what is deemed acceptable and unacceptable. Email accounts provided by iQuda are for business use only. Email carries the same legal status as other written documents and should be treated with the same care.

iQuda email users are permitted to use these resources for occasional and reasonable personal use, subject to the terms of this policy. Occasional and reasonable personal use of email is a privilege and not an entitlement. The privilege may be withdrawn at any time.

The provisions of the General Data Protection Regulations 2016 (the GDPR) and the Data Protection Act 2018, and the iQuda policies and procedures relating to data protection and confidentiality also apply to email communication. This means that emails may have to be disclosed to individuals or outside agencies as required by any legal or statutory duty imposed on the organisation.

Certain types of messages are prohibited under any circumstances: a list is provided under “prohibited use” in this policy document.

Scope

All staff employed by iQuda are responsible for ensuring that email usage within iQuda complies with this policy.

The Data Protection Officer, Garth Macintosh, is responsible for ensuring that person identifiable information is received, stored and used in line with internal policy and the General Data Protection Regulations 2016 (GDPR).

Directors and managers are responsible for ensuring that email procedures and internet access policies are known and followed in their areas.

Policy

Management of User Accounts

1. **Creation of new email accounts.** When a new employee starts work, their line manager should complete a request for a new network account and email address, if needed. This request should be sent to Managing Director Anthony Jones for approval, unless he has given prior consent.

2. When an employee or volunteer leaves iQuda, the email account will normally be disabled. Alternatively, for a limited period, the line manager may request that an alternative member of staff have access to incoming emails. In this case, the password is changed, and the email account remains live for up to three months.

Best Practice

1. **Confidential and Sensitive emails.** Confidential information can be anything that relates to clients, staff, or their families or friends, and can include: personal data; professional and contract performance data; HR information, payroll salaries and occupational health; sensitive requests, complaints, investigations, or papers for meetings that contain confidential subject matter. All iQuda email users are responsible for maintaining the confidentiality of information and complying with our policies and the General Data Protection Regulations 2016 (GDPR). Breaches of confidentiality must be reported to Garth Macintosh, the Data Protection Officer.
2. Emails containing person identifiable or sensitive data must be stored appropriately on receipt and deleted when no longer needed.
3. **Content of emails.** As all emails carry the same legal status as any written document, iQuda email users should draft emails with care, and avoid using informal, personal, disrespectful or comic language. Thought should be given to the wording used in the email, and how it might be understood by a wide range of readers.
4. **Email recipients.** All iQuda email users should take care when sending emails that the message is sent only to the appropriate individual(s). The recipients of an email should always be checked before the email is sent.
5. **Use of "Reply to All" button.** iQuda email users should consider whether it is appropriate to use the "reply to all" button. Using this function can sometimes result in a high volume of unproductive email traffic, or messages being sent inappropriately.
6. **Email Chains.** When sending an email in reply to a message received, iQuda email users should ensure that they have reviewed the entire email chain attaching to the email that they are sending. Users should take particular care not to cause damage, embarrassment or disclose confidential material to other recipients.
7. **Access to another individual's mailbox.** iQuda email users can allow colleagues access to their mailbox for operational reasons. If an employee has a planned absence, temporary sharing of mailboxes can be arranged. If an employee is away from the office unexpectedly, the employee's line manager can arrange for access to that employee's mailbox.
8. **Automatic forwarding of emails.** iQuda email users can request that their emails are automatically forwarded to a home email account, and it is the responsibility of their line manager to approve this. iQuda email users making this request should be aware that there is little security with public internet email addresses (e.g. Hotmail, Yahoo, Gmail) and that therefore additional care is required to ensure that confidential data is kept secure.

Practical Considerations

1. **Remote Access to email.** All staff with a iQuda email account can access their emails remotely via the pre-communicated methods. If you are unsure of how to access your

emails remotely, please inform the Service Desk manager. Email access is permitted through personal mobile devices, provided that you have made Anthony Jones aware of this. If you use email on your personal mobile device, you must make Anthony Aware if your phone is lost or misplaced.

2. **Auto signature and disclaimer**. iQuda have a standard signature and disclaimer that must be added to your email signature. This should not be altered in any way, Please speak to the Marketing Department who will advise you on your signature.
3. **Out of Office Assistant**. If you plan to be away from the office for more than one day, you should turn on the out of office assistant.
4. **Housekeeping**. iQuda email users should delete unwanted emails from their inbox, and make use of the filing system to store emails which may be needed for future reference.
5. **When mass mailing**, you must add details of how recipients can 'opt out' of future mailings

Acceptable Personal Use

1. The iQuda email accounts are primarily for business use. iQuda email users are permitted to use iQuda email for occasional and reasonable personal use, subject to the terms of this policy. This is a privilege not an entitlement and may be withdrawn.
2. Examples of **unacceptable** personal use:
    a. An employee uses iQuda email to forward jokes to colleagues and external recipients.
    b. An employee subscribes to forums unrelated to work using their iQuda email address.
    c. An employee replies to 15 emails throughout the day organising their social life.
    d. An employee sends a disrespectful email about a colleague, as a "joke" and copies this into colleagues and external recipients.

    iQuda email users do not have an entitlement to use email for personal use. You may be asked to justify the number of personal emails sent, and their content. Broadly, the criteria for determining acceptable personal use is similar to that of iQuda users making telephone calls of a personal nature within business hours. For example, the occasional making of necessary appointments is acceptable, while extended conversations about personal matters is not acceptable.

3. Any breach of the policy, including excessive personal use of email can result in disciplinary action up to and including dismissal, according to iQuda's disciplinary policy.

Prohibited Use

The following activities are prohibited. The following list is not exhaustive. This policy expressly forbids creating, sending and forwarding email messages which pertain to any of the following contents or activities:

1. Any pornographic, obscene, indecent or sexually explicit material

2. Breach of the General Data Protection Regulations 2016
3. Any illegal material
4. Any offensive, harassing, sexist, racist, hateful or otherwise offensive or discriminatory material
5. Chain messages and jokes
6. Any private commercial activities
7. Any fraud or criminal activity
8. Any form of defamation, discrimination, harassment or bullying
9. The introduction of viruses, spyware or malware
10. To bring the organisation or a colleague into disrepute
11. Where it interferes with the work of a colleague or the business
12. For illicitly distributing any person identifiable or business confidential material
13. For sending personal emails to a large number of recipients
14. Subscribing to non-work related forums using the iQuda email address
15. Representing personal opinions as being those of the organisation
16. Spamming or sending bulk unsolicited emails
17. For personal financial gain
18. Infringement of copyrights

Security Information

1. Passwords must be kept secure and accounts not shared. Authorised users are responsible for the security of their passwords and accounts (please see the Q204 – iQuda IT Password Policy).
2. Email accounts may be shared between users, if permitted by the account holder. In cases when a staff is unexpectedly absent from the office, access to his or her email account may be requested by his or her line manager, without reference to the member of staff.
3. All computers are secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less. Users who will be away from their desks longer than one hour should log off.
4. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses or other malware. If you are unsure whether or not an email is secure, it is best not to open it. Please clarify anything you are unsure about with a manager.
5. iQuda uses a spam filter system called MH2 to identify and reject any emails which may contain viruses or may otherwise damage the iQuda IT network.
6. All iQuda PCs and laptops have Webroot Anti-Virus installed, as a further safeguard against damage.

Implementation of this Policy

The responsibility for communicating and implementing this policy lies with the Data Protection Officer, the Managing Director and Management Team.

Enforcement

Any employee found to have violated this policy will be subject to disciplinary action, up to and including termination of contract.

Spot checks

Spot checks may be carried out at regular intervals in order to ensure compliance with this and other policies. All staff are required to take part in compliance spot checks as requested by management.