Email and Internet Policy

Introduction

The use of the email system and the internet within The Multiple Intelligence Hub (MIH) is encouraged, as this use facilitates communication and improves efficiency. Inappropriate use, however, causes problems ranging from lack of productivity to legal claims against the organisation. This policy sets out MIH's guidelines on the correct use of email and the internet, and the organisation's response to inappropriate use.

Procedure

Email

1. The email system is available for communicating matters directly concerned with the business of this organisation.

2. The style and content of email messages must be consistent with the high standards that this organisation expects from written communications.

3. To reduce email overload and aid productivity, email messages should only be sent to those employees for whom they are relevant. Send blind copies (bcc) wherever possible and do not automatically reply to all names on a "cc" list. Only send attached files where absolutely necessary.

4. Although email encourages rapid communication, the contents of email messages should be written with care as messages sent without proper consideration can cause unnecessary misunderstandings. Email should not be used as a substitute for face-to-face communication.

5. Where necessary, email messages should include a confidentiality statement.

6. All messages sent outside this organisation should include the standard disclaimer. *"Any views contained in this message are those of the author and are not necessarily those of this organisation".*

7. Employees should note that offers or contracts transmitted through email are as legally binding on the organisation as those sent on paper.

8. Email contact lists are the property of MIH even if created by the employee. Employees may not copy or remove any contact list in its entirety for use outside the organisation without the express permission of his or her Manager.

9. Any failure to follow these guidelines satisfactorily can result in disciplinary action up to and including summary dismissal.

The Internet

1. Unless it comes from an official source, information obtained from the internet (generally the World Wide Web) should be cross-checked before being used. Where that is not possible, full details of the source should be recorded.

2. Even when used for work-related purposes, browsing the Web can be highly time-consuming and therefore should be undertaken responsibly.

Unauthorised Use

1. The organisation will not tolerate the use of the email or internet system for illegal or inappropriate activities. Such activities include (but are not limited to):

    a. sending or forwarding any message that could constitute bullying or harassment (eg on the grounds of sex, race or nationality, religion, sexual orientation, age or disability)

    b. non-business use, including personal messages, jokes, cartoons or chain letters

    c. posting confidential information about other employees, the organisation or its customers or suppliers (this includes any statements posted from the employee's home computer and/or in the employee's own time).

    d. online gambling

    e. accessing offensive, obscene or indecent material, including pornography

    f. downloading or distributing copyright information

    g. sending or posting negative, abusive, rude, derogatory or defamatory messages or statements about people or organisations, including when this is done from the employee's home (or other personal) computer and/or in their own time.

2. Any unauthorised use of email or the internet is likely to result in disciplinary action, which may include summary dismissal.

Monitoring

1. Monitoring and recording of email messages and internet use will be carried out as deemed necessary. Copies of email messages will be retained as appropriate.

2. Hard copies of email messages and details of internet sites accessed may be used as evidence in disciplinary proceedings.

Security

1. All users will be issued with (or will be asked to select) a unique individual password which will be changed at regular intervals and is confidential to the user. Access to the system

using another employee's password without prior authorisation is likely to result in disciplinary action, including summary dismissal.

2. Users must take all necessary precautions against the introduction of viruses into the system.

3. Users must ensure that critical information is not stored solely within the email system. Hard copies must be kept or information stored separately on the system. If necessary, documents must be password protected.

Implementation of the Policy

1. The Project Manager or a member of the Management Team from MIH will ensure the implementation of this policy. All will be available for advice on all aspects of the policy.

2. The induction programme will include training to familiarise new employees with the email system and with internet use. Managers must ensure that all new employees receive this training and are made aware of this policy and procedure prior to using email and the internet.

3. This policy does not form part of the contract of employment and any or all of its terms may be amended from time to time.

Document Created: March 2020

Last reviewed: March 2020

Next Review Due: March 2021

Signed Managing Director:

Donna McLean