E-mail & Instant Messaging Acceptable Use Policy

Policy for acceptable use of E-mail and Instant Messaging services

An Open University Information Security Common Policy

*Open University – Information Security Team*

*Information Classification: Internal use only*
Purpose

This policy defines the security policy for E-mail and Instant Messaging in order to protect the OU’s information and systems.

Overview

This policy covers general secure practice for E-mail and Instant Messaging services and should be read in conjunction with the other IT Security Policies.

Technical terms used within this document are defined in Appendix A. The terms E-mail and instant messaging are used interchangeably in this document.

It is the responsibility of every E-mail user to know and follow this policy.

Scope

All users of OU information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1. Confidentiality

1.1 Information contained within or attached to an E-mail must be treated in accordance with the Information Classification Policy. You are expected to treat confidential E-mail information with the same care as you would with information in any other form.

1.2 You must delete any E-mails, received in error, which were intended for someone else.

1.3 Before you send a message, make sure the addressees are approved to receive the information contained in the E-mail.

2. Use of Messaging services

2.1 Care must be taken when using E-mail, as all expressions of fact, intention and opinion via messaging could be held against you and / or The Open University in the same way as verbal and written expressions.

2.2 E-mail is subject to release under the relevant sections of the Data Protection and Freedom of Information Acts. Deleting E-mails after a request has been made is an offence.
2.3 Do not send messages that might affect or have the potential to affect the performance of the Open University systems, network and / or 3rd party in any way. If in doubt please speak to the IT Helpdesk.

2.4 The University may automatically block or quarantine any E-mail identified as a potential threat to the organisation.

3. Unacceptable use

The following activities are prohibited:

3.1 Attempts to read other users’ messages without their express permission.

3.2 Auto forwarding of Open University E-mail to third party E-mail services.

4. General use and ownership

4.1 The Open University provides an E-mail & Instant Messaging service to support University activities and access is granted to users on this basis. Messages sent or received on University systems form part of the administrative records of the Open University.

4.2 Incidental and occasional personal use of the Messaging services is permitted, subject to the restrictions contained in this policy. Personal use is allowed so long as it does not cause noticeable or unavoidable cost to the University, interfere with official business or contravene any other Open University policy. Users should not use their Open University E-mail addresses for regular non-business purposes e.g. Facebook notifications.

5. Unsolicited E-mail or Junk E-mail

5.1 The Open University understands that individuals cannot control or prevent some unsolicited E-mail; however, users must not encourage others to send them such E-mails.

5.2 Some Junk E-mail can be offensive, contain links to inappropriate web sites or contain a virus. Most Junk E-mail will be filtered, however if you do receive E-mail from untrusted senders you should delete it.
6. Monitoring and Privacy

6.1 For security and maintenance purposes, authorised individuals within the Open University central IT teams may monitor all data, systems and network traffic at any time to ensure compliance with this and other security policies and the effective operation of the University’s systems.

7. Enforcement

7.1 Any breach of these policies is significant as it may undermine the effective running of the Open University and its ability to meet its duties and legal obligations. Failure to comply may lead to disciplinary action, including dismissal for serious or repeated breaches. It may also be the case that your conduct and/or action(s) may be unlawful. The Open University reserves the right to inform the appropriate authorities in such cases. You should note that you may be personally liable for actions and or conduct arising from the use of Open University Systems.
## Appendix A - Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Junk E-mail or “Spam”</td>
<td>This a term used for unwanted E-mails of both legitimate and fraudulent sources.</td>
</tr>
<tr>
<td>Computer virus</td>
<td>A computer virus is a malicious computer program that can replicate itself and spread from one computer to another</td>
</tr>
<tr>
<td>Auto forwarding</td>
<td>Capability to automatically forward E-mail onto another E-mail account immediately upon receipt.</td>
</tr>
<tr>
<td>Instant Messaging</td>
<td>Instant messaging is a form of communication that offers and instantaneous transmission of text.</td>
</tr>
<tr>
<td>Messaging</td>
<td>Method of electronic communication, typically via text. Communication may also support the attachment or sending of other media such as images, data and applications.</td>
</tr>
</tbody>
</table>