ICMP

The Institute
of Contemporary
Music Performance

Email use Policy

<table>
<tr><th>Version number</th><th>Date approved (including committee)</th><th>Reason for production/revision</th><th>Author</th><th>Proposed next review date</th></tr>
<tr><td>V1.0</td><td>Sept 2021
ExCo</td><td>Alignment with the Information Governance Framework</td><td>IT Manager</td><td>Biennially and as required</td></tr>
<tr><td colspan="5"><b>Related policies</b></td></tr>
<tr><td colspan="5">Data Protection Policy
Freedom of Information Policy
Employee Records Data Protection Policy
Records Management Policy
Data Security Policy
Acceptable Use of IT Policy
Bring Your Own Device Policy
Business Continuity Policy
Staff Disciplinary Policy
Student Disciplinary Policy
Equality & Diversity Policy
Safeguarding Policy</td></tr>
<tr><td colspan="5"><b>External Reference</b></td></tr>
<tr><td colspan="5">General Data Protection Regulation (GDPR), UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulation (PECR)</td></tr>
</table>

1. Purpose

1.1. You are reminded that e-mails are a form of written communication which is permanent, and which may be read by any member of the public. You should therefore always consider whether it is appropriate to use e-mails for the particular communication envisaged.

1.2. Please note that we may be required to disclose e-mail messages in legal proceedings relating to their subject matter and that the deletion of a message or file may not fully eliminate it from the IT Systems.

2. Scope

2.1. This policy applies to all users of ICMP's email services and therefore includes all staff, students, contractors, representatives or guests who utilise ICMP's email systems or have an assigned email account

3. Policy

3.1. If it is necessary to send sensitive or confidential information by email, then care should be taken to provide a reasonable level of protection. You should be as careful about the content of e-mails as you would be with letters. Consider in every case whether the content of an e-mail would reflect well on ICMP and, in particular, you should make sure that:

3.1.1. all contents are accurate and appropriate for dissemination by e-mail;

3.1.2. disparaging or unduly critical comments are avoided;

3.1.3. you have the authority to communicate the particular information on behalf of ICMP.

3.2. The language of any e-mails you send should be in accordance with the standards of any other written communications and at all times the language used should be appropriate to formal business communications.

3.3. You should under no circumstances use e-mails to spread gossip or similar information and the prudent test would be for you to write in e-mail form only such matters (and in such language) as would be considered suitable for a letter.

3.4. E-mail can sometimes be used as a medium for bullying and intimidating other people. This will not be tolerated. If you are unhappy about something please discuss the matter with your programme leader or academic manager, line manager or a senior manager.

3.5. If you generate or forward e-mails to others, you must be very clear as to the intended recipient. The inadvertent dispatch of material to a collective user group, for example, is no different from sending it individually to all those within that group.

4. Contracts

4.1. You should be aware that if conducting dealings with external individuals, firms, companies, organisations or institutions, and other business contacts by e-mail, you could inadvertently create a binding contract on behalf of ICMP with that external contact.

4.2. You should only deal with external contacts by e-mail if you are employed and your job requires it. All figures should be typed both in words and numbers so as to avoid expensive clerical errors. Any business e-mails should be checked before despatch as carefully as you would check a written contract containing the same matters.

5. Security

5.1. Users must not accept or open any file received as an e-mail attachment if they are in any doubt as to its source, as they may spread a virus. If in doubt, contact the IT Service desk.

5.2. Private, personal and confidential information should only be sent when absolutely necessary and under controlled circumstances (5.3).

5.3. Where it is essential to send and share confidential and personal information, the email should feature some form of security. This can include sending inside a document that is encrypted (password protected Office documents), or sending the email itself as encrypted. ICMP uses Microsoft 365 Outlook services which feature encryption to ensure that confidential or sensitive messages can only be opened by known and authorised recipients.

5.4. ICMP Email services are run on Microsoft 365's Outlook Exchange system. This system has excellent browser accessible email functionality which also has excellent Information Governance and Information Security. Using desktop applications for mail requires that the emails are downloaded to the machine, which is undesirable in both Information Governance and Information Security. Desktop applications also add an extra layer of needed IT support and can vary in capability and security functions. For these reasons ICMP officially supports and promotes the use of browser based email management and not the use of desktop applications.