new england conservatorium

Email Policy

Policy number	4.7	Version	1
Created by	HR & Operations Manager	Created on	9 September 2024
Responsible person	HR & Operations Manager	Scheduled review date	8 September 2025

1. Overview

Email has become the primary method of business communications, both within and between organisations. It is essential that email is used appropriately and securely so that it cannot compromise the security or integrity of NECOM's (the Company) data, systems or operations. For your own safety and for the safety of others, remember to exercise caution when you are communicating as a NECOM staff member with people outside NECOM. If you feel there is a problem or you feel uncomfortable with the information someone is giving you, discuss with a senior staff member.

2. Purpose

The purpose of this policy is to promote the secure and appropriate use of email within NECOM.

3. Scope

This policy applies to all employees, contractors, temporary workers and other personnel using email addresses or systems owned by NECOM or operated on behalf of NECOM.

4. Policy

4.1.1. All use of email must be compliant with the Company's policies on ethical conduct and security of business data.

4.1.2. All use of email must be in line with proper business practices and relevant to job duties.

4.1.3. The Company's email addresses or systems shall not be used for creating, distributing or accessing any offensive or illegal material, including but not limited to material with offensive comments about gender, race, age, sexual orientation or religious beliefs.

4.1.4. Any offensive material received in email must be reported to the IT Department and Human Resources without undue delay.

4.1.5. Usage of Company-owned email addresses and systems for personal use should be limited to minimal and incidental use.

4.1.6. Commercial and business related uses not part of the Company's business using Company-owned email addresses or systems is prohibited.

4.1.7. Email received to Company email addresses may not be automatically forwarded to email addresses not owned or operated by the Company.

4.1.8. Individual email addresses forwarded to email addresses not owned or operated by the Company must not contain any sensitive or confidential information.

4.1.9. The creation or forwarding of chain or joke letters from Company email addresses or systems is prohibited.

4.1.10. The Company may monitor and record any and all email messages received or sent by email addresses or systems owned or operated by the Company.

4.1.11. The Company does not necessarily monitor all email activity, but retains the right to do so.

4.1.12. If you receive an email that you suspect contains a virus, report it immediately and do not open it.

4.2. Prohibited Use

All illegal, immoral, offensive or intolerant behaviour and content are strictly prohibited on the Company email.

The following sections form a non-exhaustive list of prohibited activities and content that are expressly prohibited on the Company email.

The following activities are strictly prohibited.

4.2.1. Emailing a person with whom you are angry.

4.2.2. Not exercising caution when using email to communicate complaints or demands as it is easy to be misunderstood.

4.2.3. The use capital letters for emphasis or any other text enhancement that has the possibility of causing offence

4.2.4. Sending an email to someone who has requested that you do not do so.

4.2.5. Sending frivolous or excessive messages.

4.2.6. Sharing your username / password with a third party so they can access your email.

4.2.7. Syncing your email to a device that is not secured by a secure password (I.e. at least 12 characters, upper/lower case, numbers and symbols).

4.2.8. Flooding another email account with emails.

4.2.9. Sending an email to individual or groups whom you could not reasonably expect to welcome an email from you.

4.2.10. Obscuring the true identity of the send of the email or forging an email address.

4.2.11. Sending or requesting messages or documents that are inconsistent with NECOM policies or guidelines.

5. Compliance

5.1. Compliance Measurement

The HR & Operations Manager will verify compliance with this policy through any methods deemed appropriate, including but not limited to: business tool reports, internal and external audits and feedback to the policy owner.

5.2. Exceptions

Any exceptions to this policy must be approved by the HR & Operations Manager in advance and have a written record.

5.3. Non-Compliance

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

5.4. Reporting

If you receive an email the content of which (including an image, text, materials or software) is in breach of this policy, you should immediately report the matter to the Director and the email should be deleted. It should not be forwarded to any other person

Policy version and revision information

Policy Authorised by: GMoin

Title: Chairman of the Board