# Staff Computer & Internet Usage Policy

| | | | |
|---|---|---|---|
| Policy number | 4.4 | Version | 1 |
| Created by | HR & Operations Manager | Created on | 28 August 2024 |
| Responsible person | HR & Operations Manager | Scheduled review date | 27 August 2026 |

Purpose & Scope

The purpose of this policy is to outline the guidelines relating to NECOM staff members use of NECOM provided laptops, internet and email. This policy sets out the appropriate standards of behaviour for users accessing NECOM laptops, or when using private laptops for work related purposes.

NECOM provides internet access via Wi-Fi network, when on campus. Staff may connect to this network with private computers at their own risk. All computers connected to the network must meet the requirements of this policy. It is the users responsibility to ensure that they use NECOM internet, email and computers in a lawful and professional manner.

This Policy is to be read in conjunction with NECOM's Code of Conduct, which outlines appropriate behaviour, rights, and expectations for staff (and students). Additionally this policy is to be read in conjunction with the Cyber Security policy.

NECOM staff members are entitled to use NECOM internet, email and NECOM laptops for legitimate work related use only. Users are permitted to use internet, email and NECOM laptops for limited and reasonable personal use. However, any such use must not impact work performance or violate any part of any NECOM policies.

Guidelines

Staff must comply with the following guidelines when using internet, email and NECOM laptops:

- Users must use their own user name/ login, and their own unique password when accessing the internet, email and NECOM computer facilities
- Users must not save passwords in their browser
- Users must use multiple factor authentication when accessing NECOM data
- Users in possession of NECOM computing equipment, including but not restricted to laptop computers, must at all times ensure that it is stored or placed in areas with minimal possibility of theft or damage
- Users should protect their user name/ login details and password information at all times, and not divulge such information to any other person, unless it is necessary to do so for legitimate business reasons

- Users should ensure that they log off from internet and email, and lock the computer or shut down the computer when leaving the computer equipment unattended to ensure that others do not have access to their internet, email and computer facilities
- If a user receives an email that they suspect contains a virus, they should not open the email or attachment to the email and should immediately report the incident to their Manager and/or the HR & Operations Manager
- If a user receives an email; the content of which (including images, videos, software, materials or text) is in breach of this policy, the user must report the matter immediately to the HR & Operations Manager. The user must not forward the email to any other person. The user must not delete or move the email until the HR & Operations Manager instructs the user to do so
- Users utilising computing equipment that is not the property of NECOM to connect to the Network must:
    - 1. Maintain an up-to-date Anti-Virus program
    - 2. Ensure their firewall is turned on
    - 3. Must turn any automatic update systems to OFF. This includes System updates. Anti-Virus updates are exempted from this clause.

<u>Prohibited Conduct</u>

Staff must not send (or cause to be sent), upload, download, use, retrieve, or access any email, internet site or material on NECOM's computer network that:

- Is obscene, offensive or inappropriate. This includes text, images, sound or any other material, sent either in an email or in an attachment to an email, or through a link to a site (URL). For example, material of a sexual nature, indecent or pornographic material;
- Causes (or could cause) insult, offence, intimidation, humiliation or be construed as gossip;
- May be defamatory or could adversely impact the image or reputation of NECOM, its staff and students;
- Is illegal, unlawful or inappropriate;
- Affects the performance of, or causes damage to NECOM's computer system in any way;
- Gives the impression of or is representing, giving opinions or making statements on behalf of NECOM without the express authority of NECOM. This includes the use of social networking sites and public blogs. In addition, staff must not transmit or send NECOM's documents or emails to any external parties or organisations unless authorised to do so.

Staff must not use NECOM's computer network to:

- Violate copyright or other intellectual property rights;
- Load unauthorised software;
- Disclose any confidential information;
- Gain unauthorised access to any other computer or computer network;
- Use NECOM's facilities for personal gain (eg running a personal business).

Email Protocols

Email is provided to staff and every message you compose and send is a reflection of NECOM.

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.

When you are using your work email to send messages, please keep in mind the following:

- A disclaimer must be automatically included in all email messages, and must not be removed. *Refer to the disclaimer text below.
- Do not email a person with whom you are angry;
- Exercise caution when using email to communicate complaints or demands as it is easy to be misunderstood;
- Do not use capital letters for emphasis or any other text enhancement that has the possibility of causing offence;
- Do not send an email to someone who has requested that you do not do so;
- Do not send frivolous or excessive messages;
- Do not create, send or forward chain letters or messages;
- Do not send messages that have inappropriate content or attachments;
- Do not flood another user account with email;
- Do not send email to individual or groups whom you could not reasonably expect to welcome an email from you;
- Do not obscure the true identity of the sender of the email or forge email messages;
- Do not use any forms of obscene, harassing or abusive language on-line or in the text of your messages;
- If you suspect that an email contains a virus, do not open the email or attachment and contact reception immediately;
- 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;
- Do not send or request messages or documents that are inconsistent with NECOM policies or guidelines.

*Disclaimer text

**********

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

**********

Social Media

NECOM has an obligation to maintain a safe physical and emotional environment for staff and students. This responsibility is increasingly being linked to the use of the Internet and Information, Communication and Learning Technologies (ICLT) and a number of related cyber safety issues. The internet and ICLT devices/equipment bring great benefits to teaching and learning programs and to the effective operation of the Conservatorium.

However, it is recognised that the presence in the learning environment of these technologies (some provided partly or wholly by NECOM and some privately owned by staff, students and other members of the school community) can facilitate anti-social, inappropriate and even illegal behaviour and activities. NECOM aims therefore to maximise the benefits of these technologies whilst at the same time to minimise the dangers and manage the risks.

Social Networking Sites (SNS) include Facebook, Twitter, YouTube, MySpace, Pinterest, and LinkedIn; Blogs (Web Logs); World Wide Web (WWW) and Personal Web Sites (PWS) are to be considered as documents that are published within the public domain. Such sites allow the free sharing of information and opinions. Whilst they have their place in private life, they may be disruptive to activities at NECOM at a number of levels. Employees should not use social media for activities that may give rise to a conflict of interest between the employees' personal activities and the employer's professional activities.

Information placed on such sites may be useful, entertaining and provide a medium for friends to share experiences, photographs, messages and generally stay in touch. Conversely, entries may breach privacy conventions or regulations, may be considered "cyber bullying", may be defamatory, obscene, libellous or be of generally inappropriate content. Information published on the WWW, including that in SNS and blogs, should be considered to be permanently published.

Breach

Any breach of this policy may result in disciplinary action. If a staff member is unsure about any matter covered by this policy they should contact the HR & Operations Manager for clarification.

---

**Policy version and revision information**

Policy Authorised by:

Title:

Original issue:

**Workplace participant acknowledgement**

I acknowledge:

· receiving the NECOM Policy;
· that I will comply with the Policy; and
· that there may be disciplinary consequences if I fail to comply, which may result in the termination of my employment.

Name: _____

Signed: _____

Date: _____