Colchester Operatic Society guidance on using personal ICT equipment and handling emails

This document is for members of Colchester Operatic Society Executive Committee. It may also be relevant to members of other Society sub-committees.

Please read the below guidance on using personal ICT equipment and handling emails. All Executive Committee members are expected to read this information and agree to take personal responsibility for your own ICT equipment and its use.

Colchester Operatic Society is run by an elected committee of volunteers. As volunteers we undertake work for the Society in our own time, using our own personal ICT equipment (where necessary and appropriate) and are not paid for our roles. The Society does not provide members of the Executive Committee with ICT equipment unless in specific and agreed circumstances (for example, the membership secretary has access to a Society printer/copier in order to provide paper copies of materials for members). If committee members are asked to use personal ICT equipment above and beyond their usual role/duties then the possibility of the Society providing additional protection/alternative equipment can be discussed and/or agreed upon on an individual basis.

The Society can provide the Executive committee members with official colchesteroperaticsociety.co.uk email addresses. This gives you a level of protection from Spam/viruses as emails go through a server we pay for and that is managed. Anyone receiving public emails on behalf of COS/CO2, and therefore also has their email address published in the public domain, must use an official email address. Setting up an official email address can be organised through our webmaster, currently this is Michael Cutmore.

Anyone using their own computers for COS/CO2 emails and any COS/CO2 business using the internet is responsible for ensuring they have their own up to date anti-virus protection installed on their computers. You can get free anti-virus programmes such as Avast and Kaspersky, which have both been recommended to us by previous website and email hosts.

We strongly advise everyone to make sure they have anti-virus protection installed on their devices and run regular virus checks using their installed programmes. These programmes also need to be regularly updated. Should you discover you have got a virus on your computer at any time and this cannot be safely quarantined by your existing anti-virus protection please let the Executive committee know and we can try to find appropriate ICT advice/support to help deal with it.

To further protect yourself here is a non-exhaustive list of things (in no particular order) to do when handling emails, based on advice from various ICT professionals. We realise that you may know, and may already do the following, but it's important we officially share safe protocol to ensure all committee members are safeguarded.

- If your email provider has a virus checker, run it regularly on your mailboxes (how to do this, and if you can do this, will depend on your email provider)
- If your anti-virus programme allows you to scan your mailboxes then use that function
- Keep your anti-virus software up to date
- Act upon warnings that your anti-virus checker or email provider displays at all times, especially when opening emails

- Before opening any **attachments on emails**, safe protocol is to download them, right click on the file (viewing this from the folder you downloaded it to rather than from the tab that some browsers show downloaded files on) and select the option to run a virus checking scan before opening the file. Only open the file if the scan says it's safe to do so. We have been advised that a virus within an attachment will only be activated once the attachment is opened so downloading it is safe. If a virus is found when the file is scanned your anti-virus software should quarantine the file for you. Some email providers/programmes (such as gmail for example) automatically run virus checks on attachments but it's important to not only rely on this function, especially when receiving emails from unknown sources.
- Only click on links contained in an email if you are sure they are from a trusted source. If you hover the cursor over a link, your computer should show you the full web address for that link somewhere on the screen. Here you can see if it is taking you to where you would expect or if the web address seems suspicious - suspicious links are often very long and contain random combinations of words, letters and numbers. If in doubt don't click!
- Hackers are very clever and can send very convincing looking emails as if they are from genuine companies/banks often asking you to click on buttons/links or provide personal details. Most companies and banks will not ask you to give them details via email unless you have actively asked for a password reset or something similar. If in doubt don't click on links or provide information and contact the company/bank via another means/channel to verify the email content.
- If you think your computer has been compromised turn it off and seek ICT support

We have referred to computers throughout but this advice also applies to any personal electronic devices, such as tablets or mobiles. Though some of the checks/functions may differ for these, the principles described above are the same.

It's also important to remember that even following all this advice can not 100% guarantee a newly created virus that programmes are not yet able to identify won't find its way onto anyone's computer system but we decrease this possibility by ensuring we follow best practice.

If you have any ICT issues relating to or preventing you from completing any COS/CO2 duties, please let the Executive committee know so support can be provided.

Disclaimer

I have read the COS guidance on using personal ICT equipment and handling emails. I agree to take personal responsibility for using my own ICT equipment and ensuring safe use of this to prevent viruses and malware from corrupting my software and/or hardware. I understand that the Executive Committee are not responsible for my use of any ICT equipment, even when I am undertaking COS/CO2 duties.

Signed: _____

NB-This can be signed electronically. Date: _____