A POCKET GUIDE FOR SCIENTISTS

Safeguarding Online Communications

Brought to you by
the Climate Science
Legal Defense Fund

INTRODUCTION

Emails sent to and from scientists are increasingly subject to scrutiny through a variety of means, including aggressive open records requests, subpoenas, and even hacking. The prevalence of social media, blogs, and other digital platforms and forums has also made scientists vulnerable to new kinds of harassment and attacks.

This guide will help researchers improve their digital hygiene by providing information about how they can express their personal views and engage in activism online. It shares steps scientists can take to minimize the risks of negative consequences and how to respond to harassment.

You can always call us at the Climate Science Legal Defense Fund, where we provide free and confidential counsel to scientists facing legal attacks as a result of their work.

Contact us at (646) 801-0853

Or send an email to lawyer@csldf.org

BEST PRACTICES: EMAIL

1. Maintain a clear delineation between your professional email account—or any account affiliated with an employer—and your personal email account.

It is important to keep your professional and personal email accounts separate by conducting professional correspondence only from your professional account and personal correspondence only from your personal account.

If you are a scientist at a city, state, or federal governmental entity, at a publicly-funded institution (such as a state university), or if your work is supported by publicly-funded grants, your professional emails may be subject to disclosure under the federal Freedom of Information Act (FOIA) and state open records laws.

Each state has different laws regarding what records are protected from open records requests and what may be disclosed, so it's important to understand the rules that apply in your particular state. CLSDF has developed materials to help you understand each state's laws, take proactive measures to protect your records, and understand your rights if you find yourself the subject of such a request.

Get the information for your state at csldf.org/resources/open-records-laws/

If open records laws apply to your professional communications, know that personal emails sent to or from your professional account can potentially be subject to public disclosure in response to an open records request. Similarly, if you regularly send or receive correspondence related to your professional activities from a personal email account, it may be subject to open records requests.

Minimal use of your personal account for professional correspondence is unlikely to open up your personal account to open records requests. Nonetheless, we recommend that you avoid such a practice. We also recommend that you avoid forwarding professional emails to your personal account and vice versa. This too will help ensure that your personal correspondence stays private.

BEST PRACTICES: EMAIL (CONT.)

2. Use your own equipment and devices for personal communications.

Send and receive personal communications only on or from your personal computer, phone, or other device. Do not use employer-issued equipment for such communications.

State laws vary on the extent of an employer's right to access electronic communications conducted using the employer's equipment. The bottom line is that the law generally offers only limited privacy protection for communications sent or received using an employer's computers, even if the messages are sent or received by a private personal account. The same is true for text messages and even phone calls and voicemails involving an employer-issued phone or device.

3. Learn your employer's email retention policies—and follow them.

Your employer likely has explicit records retention policies, whether you work for a government entity or a private enterprise. These policies will detail how long your professional emails and other records should be kept before they are deleted or archived, or at when your employer will proactively delete or archive such records.

Such policies are meant to ensure that the company or institution engages in adequate and appropriate record keeping, while simultaneously making certain that records that are no longer needed are discarded. Consistently following such a policy will help make sure you're in compliance with your employer's standards.

If your employer does not have such a policy, you may choose to discard old emails that are no longer necessary after a certain point in time. For example, eliminating unneeded emails after three years—the general rule of thumb for the amount of time the IRS has to audit a tax return—may be appropriate.

Be aware that this practice has downsides. Only discard records you're sure you will never need again, and be mindful that an overly aggressive deletion policy does not always reflect favorably on the account holder even when entirely legal. Moreover, records may remain on a server even after being deleted from an individual account.

4. Beware of the "reply all" and "forward" buttons.

You can reduce risk simply by limiting the number of recipients on the emails you send. Consider not replying all or forwarding email to large groups from your professional email account unless it is truly necessary. Among other things, it is important to remember that even if you are not personally subject to open records laws or other legal inquiry, one of your correspondents may be.

Also be mindful of the content and tone of your emails, and think carefully before writing about certain topics. Sensitive issues may be best discussed in person or over the telephone. Ill-advised messages can come back to haunt the writer in a number of ways, usually by your words being taken out of context.

BEST PRACTICES: SOCIAL MEDIA AND OTHER ONLINE PLATFORMS

Be mindful of what you share and how you engage.

We're all familiar with the instant furors, Twitter wars, and public shaming that can result from a controversial blog post or ill-conceived tweet. You should also remember that these events can have employment consequences: It has become a fairly common occurrence for employees to be disciplined or fired because of something they post online.

But scientists—even those employed by government agencies or publicly-funded research institutions—have a general right to express personal views and engage in activism online. Striking the balance between exercising that right and avoiding unwanted spotlights that social media may create comes down in no small part to your personal risk preferences.

These approaches can help minimize any negative impacts in the workplace for scientists writing blogs posts, and using social media or other platforms.

- Employers, including government entities, usually have explicit social media policies. If your employer has such a policy, familiarize yourself with it and follow it.
- When posting to a personal social media account or blog, keep in mind that your employer may be aware of what you are posting. Privacy settings may not succeed in creating the intended privacy and even "anonymous" posts often are not really anonymous—or they do not stay that way. Consider your employer's likely reaction and weigh costs and benefits before proceeding.
- Conduct any personal social media communications on your personal accounts, not your employer's, and do so in a way that doesn't give the impression you're speaking on behalf of your employer.
- Consider not listing your employer affiliation on your private social media accounts. This will help clearly delineate them as private accounts used to express your personal views.

- Use your personal contact information when signing petitions, op-eds, open letters, and other documents that reflect your personal views.
- Consider using disclaimers such as, “These are my personal views, not those of [my employer],” or “Title and affiliation for identification purposes only.”

If you become the recipient of harassing messages online, the best option may be to not engage. Look for signs that the sender is wasting your time or seeking to provoke you with “gotcha” questions or inflammatory statements. Ignore and archive emails if there are signs they were sent in bad faith. An attacker may be seeking to rattle you, use your response in an attempt to malign you publicly, and/or use your response as a launch pad to further harass you.

The Climate Science Legal Defense Fund produced this guide to help scientists understand how to manage their online communications. This guide concerns only U.S laws, and nothing in it should be construed as legal advice for your individual situation.

CSLDF provides free counsel to scientists facing legal issues as a result of their work. Contact us at **(646) 801-0853** or email **lawyer@csldf.org** to arrange a free and confidential consultation with an attorney.

The Climate Science Legal Defense Fund (CSLDF) works to protect the scientific endeavor by helping defend climate scientists against politically and ideologically motivated attacks. CSLDF is a non-profit organization under section 501(c)(3) of the Internal Revenue Code.

To view additional CSLDF guides and resources, scan the QR code or visit https://www.csldf.org/resources

Location
New York, NY

Website
csldf.org

Find this guide online at:
csldf.org/resources/pocket-guide-to-safeguarding-online-communications