WOMEN IN HIGHER EDUCATION

IN HER OWN WORDS: Keep Your Personal Email Personal

Dr. Katie Rose Guest Pryal JD tells readers that most of us don't pay attention when we use institutional technology to handle our private business.

We working women often find ourselves fitting the work of home into the margins of the work at our institutions. As we dash across campus to a meeting, we phone the pediatrician to schedule an appointment. While we're waiting to meet with a student, we email the house painter to finalize a budget. We pay the power bill online using the browser on our work computer.

Technology is a great tool to help us make the most of those small margins. Technological methods of communication like email, text and instant messaging, often make the difference between meeting our nonwork obligations and failing to. Most of us don't pay attention when we use institutional technology to handle our private business. I'm writing to advise you to pay attention.

Right to know?

Whether you work for a public or private institution, an employer almost always has the right to access your institutional email and to access data on institutional devices. This rule holds true for institutions of higher learning, as some Harvard employees learned last year.

And if you work at a public institution, you might have heard of the federal Freedom of Information Act (or "FOIA") and the state-level statutes that parallel this federal statute. These statutes give members of the public the right to access the documents of public employees for almost any reason.

For example, the North Carolina Public Records Law covers "all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics"—a broad swath of data. If any of this data was "made or received…in connection with the transaction of public business by any agency of North Carolina," then the documents are subject to a public records request. (To compare, the New York law is very similar.)Anything you type into your institutional email account, text on your institutional mobile phone or save on the hard drive of your institutional laptop is potentially accessible either by your employer or under a state public records law. If such worries seem unwarranted, or even paranoid, consider the following.

First, the American Association of University Professors (AAUP) has already considered these risks. In its statement on Academic Freedom and Electronic Communications, the AAUP warns that our multidevice campus lifestyle can "blur boundaries between communications activities" that are for home and for work. Furthermore, "Digital devices such as smartphones [are] permitting users to create their own content but also to leave personal 'footprints,' which might be subject to surveillance"—surveillance by your employer, or by the public via public records request.

Second, New York Times columnist Paul Krugman condemned a high-profile public records attack against William Cronon, a history professor at the University of Wisconsin who published a letter criticizing his state's Republican governor. After the letter's publication, Cronon received a "demand for copies of all e-mails sent to or from Mr. Cronon's university mail account containing any of a wide range of terms, including the word 'Republican' and the names of a number of Republican politicians." This records request gives you a sense of how broad the requests can be.

Lastly, a colleague of mine was slapped with a public records request by a political lobbying group that disagreed with his extracurricular activist work. (And then, covering my colleague's story, our local newspaper accessed emails of a variety of administrators across campus.) Once my own division was targeted, I knew I needed to learn how to protect my privacy.

Know your risk

You know those emails that your uncle constantly forwards to your family, full of inflammatory language? The ones you just delete without reading? Those are sitting in your university email account subject to a keyword search by (1) your employer, who technically owns your email, and (2) members of the public who make records requests. When they sift through your email looking for their keywords, they can find information about your children.

Your privacy is vulnerable. But it's easy to protect it if you just take a few precautions.

• Email. The easiest way to protect the privacy of your email is to create an offsite email account for personal work. Gmail is a good choice. You can set your devices to gather email from both of your accounts. You'll need to practice switching back and forth between your private email and your work email to keep your communications separate.

• Devices. When my colleague was targeted, the public records request not only asked for his institutional emails, but also any emails and messages sent from a device provided by the institution. Plus, at any point, your employer may access your institutional devices: laptop, tablet and phone. So, if you can afford to, purchase your own devices and use them instead.

If you can't afford to purchase your own devices—or if you aren't allowed to use them—use settings to protect your privacy. For example, always set your browser to clear history, cookies and passwords when you quit the program (and then always remember to quit the program when you leave for the day). You'll need a secure way to remember your passwords, but you shouldn't store your passwords on your institutional computer anyway.

It'll take some time to build these new technology habits. However, after you've consolidated your private business on private platforms and devices, your private life will not only be more secure, but it will also be more portable, should you ever need to make a career change.

Dr. Katie Rose Guest Pryal, JD *is an author and freelance writer who covers health, higher education, motherhood and careers, though not necessarily together. She's active on Twitter (@krgpryal), Facebook (facebook.com/katieroseguestpryal), and her blog (katieroseguestpryal.com). She teaches at the University of North Carolina at Chapel Hill.*

—

Guest Pryal, Katie Rose. *IN HER OWN WORDS: Keep Your Personal Email Personal.* **Women in Higher Education** 24(1), 16 and 19.