Auto-Forwarding emory.edu Email and LGS Students

August 8, 2013

Many graduate students want to auto-forward email sent to their emory.edu addresses to another email address and system. This practice raises concerns about information security and reliability, as well as some issues related to convenience and privacy. Below is our policy on auto-forwarding, along with some considerations relevant to the policy and to making an informed decision about auto-forwarding.

LGS Policy

- LGS students are permitted to auto-forward email in accordance with Emory University’s Policy 5.13 Automatic Forwarding of Email from the Emory Exchange Environment (see http://policies.emory.edu/5.13).

- Graduate students must renew their request for auto-forwarding annually. Once a year, LGS and University Technology Services (UTS) will request that LGS students who are auto-forwarding their email complete a new auto-forward request. If a student does not complete the request, UTS will rescind the auto-forwarding and create an Office 365 account to receive emory.edu email.

- The renewal requirement seeks to ensure that graduate students whose circumstances have changed since their previous request, and who no longer meet the conditions specified in the request form, will discontinue their auto-forward.

Auto-Forwarding at Emory

It’s helpful to understand what auto-forwarding means in the Emory context. Auto-forwarded emails are not first received into an emory.edu email account and then passed on, but are instead simply deflected to the forward-to address. Emory’s email system does not allow a user to configure it to forward all emails received to another address. This limitation is part of the security measures built into the system. Instead, if an auto-forward is granted, that user’s Emory email account is deleted, and all emails sent to the user’s emory.edu address are passed on to the auto-forward address. Beyond the fact that they were passed along, no records of such emails or their content remain in an Emory system.

Information Security

Emory’s email systems are designed to provide a secure environment that makes it possible to send confidential and sensitive information via email. Any time email is forwarded outside the emory.edu systems, those security measures cease to apply. Many graduate students will be dealing with protected information that should remain inside the emory.edu systems.

Much of Emory’s concern is structured by two overarching legal frameworks: FERPA and HIPAA, which govern how Emory must treat information related to students and patients.

- FERPA (Family Educational Rights and Privacy Act) is the Federal law that provides specific rights to students regarding their educational records. You can learn about FERPA here http://www.registrar.emory.edu/students/ferpa.html.

- HIPAA (Health Insurance Portability and Accountability Act) provides standards and rights for patients regarding their personal health information, and details the specific technology security
protections all health care organizations must undertake to ensure confidentiality of patients’ medical information. You can learn about HIPAA here https://hipaa.emory.edu/home/index.html.

Emory’s email systems are FERPA and HIPAA approved. Gmail, yahoo, mac, etc. are not.

During the course of their careers at Emory, many graduate students will work with information that falls in categories defined and protected by FERPA and HIPAA – the former more likely than the latter. This can happen in the context of teaching and research, or in the context of part time work at Emory that many graduate students take on at various stages of their careers.

Just about any graduate student may work with protected information. Students in college-aligned programs are the most likely to deal with FERPA protected information, and students in programs where research engages with clinical data are the most likely to deal with HIPAA protected information. But because teaching and research projects vary widely, and because students often take part time jobs across the whole of Emory, it is difficult to predict which graduate students will in fact deal with protected information.

If information protected by FERPA or HIPAA is sent to a graduate student’s emory.edu address and auto-forwarded to another email provider, then Emory’s obligation to protect and secure such information has been violated in that particular case.

Information Reliability

Emory supports the systems associated with emory.edu addresses (Exchange and O365), and emails sent and received within those systems can be tracked, are archived, and so on. When email is auto-forwarded to an outside provider, that support ends, and Emory is not responsible for any support, tracking, delivery logs, archiving, etc.

Auto-forwarding sometimes creates reliability issues. When you send to emory.edu addresses from a Gmail or other account, your email may get caught by Emory junk filters, and vice versa. This sometimes happens because auto-forwarded emails may be associated with two addresses (the emory.edu address and the auto-forward address) in ways that filters interpret as associated with spamming. Other times it happens for reasons that are difficult to trace or remedy, like which servers emails pass through and what else those servers are used for.

These issues are not very common, but they do occur. If they cause significant emails to or from an auto-forward address to be diverted, then Emory is not responsible for such failures or for any remedies required to address them.

Convenience

It is attractive to consolidate all emails to one system, particularly if that system supports calendaring, file storing and sharing, and more. But on balance, the convenience issue may be more complicated.

First, if you auto-forward, then your entire Exchange or O365 account is deleted. This has a couple of consequences:

- Any existing emails at the emory.edu address will be deleted.
- Your email system will not be linked to Emory’s directory.
- Without an Exchange or O365 account, you cannot access Emory’s calendars – cannot access shared calendars and cannot participate in generic calendars.
• Meeting planning with Emory Exchange or O365 users will likely function across platforms, but will be subject to some limitations and bugs.

Second, as Emory moves fully to the O365 environment and expands the features accessible within the emory.edu systems, you may find that not having an O365 account reduces your ability to share information with Emory colleagues. Emory is currently in the process of moving all emory.edu users into Microsoft Office 365. At present, Emory’s O365 features center on email and calendaring, but in the future available features will expand to include messaging, cloud-based file sharing, and more. Without an O365 account, your ability to participate in these will be limited both by cross-platform constraints and by the security measures that surround the emory.edu systems.

Personal and Professional Information
Navigating the lines between personal and professional information in the digital realm is complicated, and we find that Emory colleagues manage this in many different ways. As you make your choice, consider some ways in which your choice affects your information privacy.

On the one hand, using Emory systems for personal information makes that information subject to Emory policies and conditions. It may be helpful to read Emory's Information Technology Conditions of Use Policy, [http://policies.emory.edu/5.1](http://policies.emory.edu/5.1). On the other hand, using your personal email system to conduct your professional Emory life may expose you to risks you prefer to avoid. You may find yourself responsible for violating Emory’s FERPA or HIPAA policies, or for losing important information because a commercial system crashed or was otherwise compromised. If you become involved in problems like research misconduct or plagiarism (rare, but it does happen), perhaps as a witness or teacher, you may find investigations reaching into your personal information in unwanted ways.

– Approved August 8, 2013