Report of the E-mail and Research Privacy Task Force
George Mason University

FINAL REPORT 3 April 2013

Contents
1 Introduction
   1.1 The challenge of e-mail and research privacy
   1.2 Precipitating events
   1.3 Charge from the Faculty Senate
   1.4 Documents
   1.5 Interviews
2 Findings
   2.1 Virginia’s laws and policies limit the privacy protection the university can offer its faculty and staff
      2.1.1 Virginia Department of Human Resource Management Policy 1.75 – Use of Electronic
           Communications And Social Media
      2.1.2 Virginia Freedom of Information Act (Code of Virginia, Chapter 37 of Title 2.2)
      2.1.3 Public Records Act (Code of Virginia §§ 42.1-76, et seq.)
   2.2 Commonwealth universities do have choices to make within the confines of state law
   2.3 George Mason University Policy Number 4011 also affects e-mail and research privacy
   2.4 Features of the Office 365 system increase the likelihood that e-mail will be viewed by someone
      other than the sender and recipient.
      2.4.1 The university plans to configure the Office 365 system to store all messages for three years
      2.4.2 The Office 365 system will allow searches across accounts
      2.4.3 These features may result in greater inspection and release of employee e-mail
3 Recommendations to state officials
   3.1.1 The General Assembly should consider modifying the Freedom of Information Act to
distinguish official and non-official correspondence
   3.1.2 The Library of Virginia should reach out to university faculty as it revises its retention
schedules
   3.1.3 The Department of Human Resource Management Should Reconsider Policy 1.75, "Use of
Electronic Communications and Social Media"
4 Recommendations to George Mason University officials
   4.1 General policies
      4.1.1 Mason should adopt a general privacy policy for electronic communications
      4.1.2 The Office of University Counsel should specify procedures for monitoring electronic
communications
      4.1.3 The university should consider privacy interests as it revises policy 4011
      4.1.4 The provost and deans should train promotion and tenure committees
      4.1.5 The university should consider alternative communications systems for human subjects
research
   4.2 Freedom of Information Act policies
      4.2.1 Mason should revise Policy 1117 (Responding to Virginia Freedom of Information Act (FOIA)
requests for records) to codify the FOIA Compliance Officer’s actions in response to a FOIA request.
      4.2.2 The FOIA Compliance Officer should produce an annual report
      4.2.3 The university counsel should defend assertions of exclusion
   4.3 E-mail policies
      4.3.1 The university should explain how faculty and staff e-mail is stored
      4.3.2 The university should establish separate e-mail accounts for student-employees
      4.3.3 The university should consider establishing separate e-mail accounts for faculty who serve in
administrative roles
      4.3.4 The university website should alert potential correspondents that their messages may be
retained and shared
      4.3.5 The university should consider appending information to outgoing e-mails
      4.3.6 The university should seek ways to inform faculty and staff about Virginia laws and policies
and about their implications for the use of electronic communications
4.3.7 The university should consider delaying the implementation of the litigation-hold feature.

4.4 Recommendations to department chairs
   4.4.1 Department chairs should establish procedures for records management and communicate them with their faculty.
   4.4.2 Department chairs should explain to promotion and tenure committees and to faculty their responsibility to preserve records and the limits of those records’ confidentiality.

5 Recommendations to individual faculty, staff, and student workers
   5.1 Mason faculty and staff should use Mason e-mail accounts for transacting public business.
   5.2 Mason faculty and staff should avoid using Mason e-mail accounts for personal correspondence.
   5.3 Mason faculty and staff should consider using alternative e-mail accounts for some professional and scholarly correspondence.
   5.4 Faculty and staff could consider using signature files to remind themselves and alert correspondents to confidentiality limits.
   5.5 Researchers who collect sensitive information about human subjects should consider alternatives to e-mail.
   5.6 Faculty and staff should act professionally in all their professional activities.
1 Introduction

1.1 The challenge of e-mail and research privacy

As employees of a public university, George Mason University faculty and staff are both civil servants and members of a scholarly community. While they take pride in serving the Commonwealth and in pursuing knowledge, they at times face tension between these two roles. Laws preserving public records and providing access to them are essential to democratic government. On the other hand, as the University of Virginia recently argued, “If public university faculty in Virginia no longer enjoy a zone of privacy around their scholarly communications, the ability of the Commonwealth’s schools to continue to attract and retain the best and brightest scholars from around the world—a creative engine that drives a huge and growing portion of Virginia’s economy—will be damaged.” State legislators, officials, and courts, and Mason administrators, faculty, staff, and students share the common challenge of balancing the public’s interest in openness with its interest in fostering the freedom of thought and expression.

This report seeks to explain existing laws and policies concerning faculty and staff e-mail and research privacy. It suggests ways that members of the Mason community can act appropriately within existing rules as well as ways those rules might be modified to the benefit of all.

1.2 Precipitating events

In spring 2013, George Mason University will adopt a new e-mail system for faculty and staff, known as Office 365, to replace the previous system, known as MEMO.

This transition comes during a period of heightened interest in the privacy of electronic communications by university faculty, staff, and administrators. In recent years, activists and journalists have used state freedom of information laws to seek unprecedented access to the e-mail accounts of faculty and visitors at public universities in Michigan, Wisconsin, and Virginia, including Mason. In spring 2013, newspapers reported that Harvard administrators had searched the subject lines of e-mails sent by a group of deans without notifying them. Such events highlight the need for university administrators, faculty, and staff to develop a shared understanding of what constitutes appropriate use of university-provided electronic communication tools.

1.3 Charge from the Faculty Senate

On October 10, 2012, the Faculty Senate established the E-mail and Research Privacy Task Force with the following charge:

1. Clarify George Mason University’s policies and current practice regarding access to and use of faculty and staff e-mail, archived information (electronic or otherwise) and access to and use of faculty research data.

2. Investigate relevant policies from institutions of higher education within the Commonwealth of Virginia, within George Mason University’s set of peer institutions, and perhaps others that have taken the lead on this issue.

3. Gather information relevant to these issues from involved organizations such as the American Association of University Professors.

---

1 Respondents’ Joint Memorandum In Opposition to Petitioners’ Verified Petition for Mandamus and Injunctive Relief, American Tradition Institute v. University of Virginia, 24 July 2012.

5. Provide specific recommendations for amending existing policies or creating new policies that offer substantive protection of faculty and staff e-mails and faculty research data, including but not limited to situations, criteria and processes for justifying and informing faculty and staff about internal administrative or supervisor access, law enforcement access, and access by external agencies or individuals.

1.4 Documents

The task force reviewed relevant laws and policies of the Commonwealth of Virginia, policies of Mason and other Virginia public universities, court cases, rulings of the Virginia Freedom of Information Advisory Council, documents produced by the American Association of University Professors, and news accounts of controversies at Mason and other universities.

1.5 Interviews

The task force met in person and corresponded with the following university officials:

• Aurali Dade, Assistant Vice President for Research Integrity & Assurance
• Veronica Fisher, University Records Manager
• Philip Hunt, Director of Development for Access Initiatives and FOIA Compliance Officer
• Thomas Moncure Jr., University Counsel
• Walt Sevon, Deputy CIO & Executive Director, Technology Systems Division

All of these officials were generous with their time and helpful and candid with their answers to our questions. We are most grateful for their assistance.

In addition, Madelyn Wessel, Associate General Counsel, University of Virginia, was most helpful in helping us understand the case of American Tradition Institute v. University of Virginia.

2 Findings

2.1 Virginia’s laws and policies limit the privacy protection the university can offer its faculty and staff

Three state laws and policies are particularly relevant to the questions of e-mail and research privacy. University officials have crafted policies to comply with these laws and policies, and any revision to those university policies must respect them as well.

2.1.1 Virginia Department of Human Resource Management Policy 1.75 – Use of Electronic Communications And Social Media

This policy instructs that

No user shall have any expectation of privacy in any message, file, image or data created, sent, retrieved, received, or posted in the use of the Commonwealth’s equipment and/or access. Agencies have a right to monitor any and all aspects of electronic communications and social media usage. Such monitoring may occur at any time, without notice, and without the user’s permission.\(^4\)

As an agency of the state, the university cannot create any legal rights or expectations of privacy. It can, however, spell out the circumstances under which it will use its authority to monitor communications, as has Virginia Tech (see below).

2.1.2 Virginia Freedom of Information Act (Code of Virginia, Chapter 37 of Title 2.2)

The Virginia Freedom of Information Act (FOIA) states that "Unless a public body or its officers or employees specifically elect to exercise an exemption provided by this chapter or any other statute, every meeting shall be open to the public and all public records shall be available for inspection and copying upon request. All public records and meetings shall be presumed open, unless an exemption is properly invoked."

The Virginia Freedom of Information Advisory Council, which interprets the act, has stated that "A public body must provide electronic records in any medium identified by the requester, if that medium is used by the public body in the regular course of business." 5

FOIA does list exclusions, including several specific to educational institutions (§ 2.2-3705.4). The most relevant for the work of the task force is subparagraph(4), the exclusion for

Data, records or information of a proprietary nature produced or collected by or for faculty or staff of public institutions of higher education, other than the institutions’ financial or administrative records, in the conduct of or as a result of study or research on medical, scientific, technical or scholarly issues, whether sponsored by the institution alone or in conjunction with a governmental body or a private concern, where such data, records or information has not been publicly released, published, copyrighted or patented.

In September 2012, the Prince William County Circuit Court ruled that the University of Virginia could use this provision to deny a request for the e-mail correspondence of a former faculty member. 6 In an oral ruling, Judge Sheridan held that

Subparagraph (4), the exclusion in question, does arise from the concept of academic freedom and protection of research. Early research, we all know, would be protected for a variety of reasons. The concept of churn of intellectual debate, evolving research, suddenly going up a dead-end street in your paths, having the ability to come back, re-look at it, go through a period . . . look back at it again and find a different opinion, all that is part of the intellectual ferment that is protected, in my view, by subparagraph (4). 7

However, FOIA states that such records and other excluded records “may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law.” Thus, though it has been Mason’s practice to assert exclusion whenever possible, the university cannot promise faculty and staff that it will not release excluded records in response to a FOIA request.

2.1.3 Public Records Act (Code of Virginia §§ 42.1-76, et seq.)

The Public Records Act states that

No agency shall destroy or discard a public record unless (i) the record appears on a records retention and disposition schedule approved pursuant to § 42.1-82 and the record’s retention period has expired.

---

7 American Tradition Institute v. University of Virginia, Partial Transcript (Circuit Court of Prince William County 2012).
The relevant retention and disposition schedule is Library of Virginia General Schedule 111: All State Supported Colleges and Universities, College And University Records (GS-111). In some cases, this refers to General Schedule 101: All State Agencies, Administrative Records (GS-101).

Of particular importance to question of privacy are the instructions for “Offices of Presidents, Vice Presidents, Provosts, Deans, Department Heads, and Boards of Visitors,” which governs “the incoming and outgoing correspondence of college or university officials. Includes but is not limited to letters, memoranda, fax transmissions, and related attachments in any physical form including paper or e-mail.” The schedule refers to GS-101, which in turn requires most correspondence to and from department or division heads to be preserved for three years. Thus, the university is required by law to preserve the official e-mail of university department and division heads for three years.

GS-111 also requires that “the actual research conducted by a college or university employee. Includes, but is not limited to, notes, notebooks, drawings, Work papers, technical data, experimental results, statistics, findings, and conclusions” be preserved for three years and then offered to the university archives if sponsored by the college or university, five years if contract or grant funded.

The status of faculty correspondence and records under public records laws is uncertain. Mason employs its faculty with the expectation that they will pursue scholarly activities, but, as the university counsel has explained, an expectation is not the same as a job requirement. (Faculty conducting research within the context of a sponsored project may occupy a different position in regard to the definition of the transaction of public business.)

A Virginia Freedom of Information Advisory Council precedent supports this view. In 2010, a reporter filed a FOIA request for records related to a report authored by two faculty members. The Virginia Freedom of Information Advisory Council deemed those records not subject to FOIA on the grounds that they did not constitute the transaction of public business:

The report was commissioned by and presented to Congress, not by the University. The professors and the University have asserted in the response to your request that the work performed was not part of the professors’ duties at the University. Therefore the records are not in the transaction of the University’s or the professors’ public business.8

On the other hand, the Prince William Circuit Court has ruled that academic research is a governmental action “when it is done by government employees on government property using government facilities for government purposes and/or other matters related to his status as a faculty member.”9 The court rejected the arguments by Professor Michael Mann’s lawyer that the professor’s e-mails were not public records. Nationwide, the question remains unsettled.10

2.2 Commonwealth universities do have choices to make within the confines of state law

A Commonwealth university cannot offer its employees more legal rights than are provided by state law. It can, however, adopt policies on how it will exercise its own legal rights.

For example, the University of Virginia policy on “Monitoring and Review of Employee Electronic Communications or Files” states that “The University holds as core values the principles of academic freedom and free expression. In consideration of these principles, the University will not monitor the content of electronic communications of its employees in most instances, nor will it examine the content of employee electronic communications or other employee electronic files stored on its systems except under certain circumstances.”11

9 American Tradition Institute v. University of Virginia, Partial Transcript (Circuit Court of Prince William County 2012).
Similarly, in 2005, the Virginia Polytechnic Institute and State University (Virginia Tech) adopted its “Privacy Policy for Employees’ Electronic Communications.” While not guaranteeing the privacy of any communication, this policy reduces the chance that employees’ e-mails and other records will be arbitrarily viewed. This policy, which appears to have been vetted by university counsel at Virginia Tech, could serve as a model for Mason.

2.3 George Mason University Policy Number 4011 also affects e-mail and research privacy

University Policy Number 4011: Ownership and Maintenance of Research Records states that research records created “within the scope of an individual’s employment or enrollment at the university” “are the property of George Mason University.” This includes some work by students, including a record that “relates to a report intended for publication or dissemination in which the student’s affiliation with the university is stated.” This policy was approved on 20 November 2008 and includes a provision that it will be reviewed every five years or sooner.

2.4 Features of the Office 365 system increase the likelihood that e-mail will be viewed by someone other than the sender and recipient.

2.4.1 The university plans to configure the Office 365 system to store all messages for three years

The MEMO e-mail system uses backup tapes but maintains them for only 60 days. Under current plans, the Office 365 system will make copies of all messages sent to and from accounts by all faculty and staff (except for wage and student-wage employees), and preserve those copies for three years. This is known as the “litigation hold” feature, since it was designed to allow enterprises to preserve records that might be subject to discovery as a result of litigation. Even if a faculty or staff member deletes a message from his or her account, a copy will remain in the three-year archive. The message will also remain even if a faculty or staff member leaves the university during that time. Microsoft charges $1 per month for each account with this feature.

The committee in charge of selecting a new e-mail system chose this design in order to comply with the Public Records Act by preserving all department and division head correspondence for the three years required by GS-101.

2.4.2 The Office 365 system will allow searches across accounts

Under the MEMO e-mail system, if an e-mail account must be searched for legal, audit, or FOIA purposes, only one account can be searched at a time. Office 365 allows users with certain privileges to search across multiple accounts at once. Designated personnel in the Office of University Counsel will be given these privileges.

2.4.3 These features may result in greater inspection and release of employee e-mail

Members of the Office of the University Counsel do not routinely read employee e-mail, but they do have the responsibility to read e-mail when required by law or state policy. Both of these features of Office 365 may require them to inspect more e-mail than before, because broader searches will be possible.

Under the MEMO system, if a faculty or staff member deletes an e-mail, in 60 days that message disappears from the sender’s account and cannot be produced in response to audit, investigation or FOIA requests. The three-year archive feature will, of course, greatly extend the period in which a message is subject to scrutiny.

Also, under the MEMO system, the faculty or staff member whose e-mail is being requested can be presumed to have the most complete copy, and it is the practice of the FOIA compliance officer to request

12 http://www.policies.vt.edu/7035.pdf
13 http://universitypolicy.gmu.edu/policies/ownership-and-maintenance-of-research-records
documents from the holder of the e-mail account. Under the Office 365 system, the three-year archives may constitute a more complete record of a faculty or staff member’s e-mail, and the FOIA officer may need to present search requests to the Office of University Counsel.

Finally, FOIA requestors may begin to make requests for messages sent to and from large numbers of accounts, rather than seeking the e-mail of only one or two faculty members, as has been the case in highly publicized cases in Virginia and elsewhere. Under the MEMO system, the labor required to perform multiple searches may have made such requests prohibitively expensive to the requestor, but the new search function may greatly reduce this barrier.

Even if a record is ultimately judged not to be subject to FOIA or is otherwise released, making that determination may require a loss of some confidentiality. For example, in May 2011, the University of Virginia agreed to allow petitioners’ counsel to review documents that the university claimed were exempt from FOIA.  

Again, we expect Mason administrators to honor faculty and staff privacy to the best of their abilities, but those abilities are somewhat diminished by features of the new system.

3 Recommendations to state officials

Because state laws and policies shape the decisions made by university employees, the Faculty Senate may wish to consider passing on these recommendations to the appropriate state officials.

3.1.1 The General Assembly should consider modifying the Freedom of Information Act to distinguish official and non-official correspondence

The September 2012 Prince William Circuit Court ruling in American Tradition Institute v. University of Virginia appears to exclude most faculty correspondence from FOIA requests. However, this exclusion could be clarified in a revision of FOIA itself.

In response to a Freedom of Information Act request for a faculty member’s e-mails, University of Wisconsin Chancellor Biddy Martin explained, “When faculty members use email or any other medium to develop and share their thoughts with one another, they must be able to assume a right to the privacy of those exchanges, barring violations of state law or university policy. Having every exchange of ideas subject to public exposure puts academic freedom in peril and threatens the processes by which knowledge is created.” This wisdom should be encoded in Virginia law. One report notes Utah’s law as a particularly promising model.

3.1.2 The Library of Virginia should reach out to university faculty as it revises its retention schedules

The Library of Virginia’s Records Retention and Disposition Schedule General Schedule No. 111: All State Supported Colleges and Universities: College and University Records lists several categories of records that academic departments and perhaps individual faculty are required to retain for varying lengths of time. We understand that the Library plans to revise this schedule with input from university records managers, and we hope it will seek input from faculty members—including the Virginia Conference of the AAUP—as well.

16 Levinson-Waldman, Academic Freedom and the Public’s Right to Know, 12.
3.1.3 The Department of Human Resource Management Should Reconsider Policy 1.75, “Use of Electronic Communications and Social Media"

As noted above, this policy states that “no user shall have any expectation of privacy in any message, file, image or data created, sent, retrieved, received, or posted in the use of the Commonwealth’s equipment and/or access.” This is a sweeping policy whose justification is unclear. A narrower policy could lay out the situations in which monitoring might be justified.

4 Recommendations to George Mason University officials

4.1 General policies

4.1.1 Mason should adopt a general privacy policy for electronic communications

Some universities have adopted clear privacy policies for electronic communications, and we recommend one for Mason.

We would like such an electronic communications privacy policy to be specific about:

• which personnel will have the computer privileges to search employee e-mail.

• under what circumstances they will read employee e-mail.

• what steps they will need to take. For example, they might be required to log all such searches, describing when they access records and what was searched.\(^{17}\)

• what notification employees can expect if their e-mail is read. We assume that Mason personnel will be notified if their e-mail is searched. Furthermore, we hope that advance notification would be the norm, and only under exceptional circumstances, such as an ongoing criminal investigation, would such notification be delayed until Mason was alerted that such investigation had concluded.\(^{18}\)

Because it was written with the requirements of Virginia law in mind, Virginia Tech’s policy is a particularly useful model. That policy states that “the university does not routinely monitor or access the content of electronic communications, computer files, or voice mail of its employees, whether stored on university equipment or in transit on the university network.” Instead, it delimits specific circumstances—such as responses to FOIA requests, approved audits, and emergency situations—in which employee communications may be monitored and procedures for requesting access for other situations.

Additional criteria are recommended in the AAUP’s 2004 report, “Academic Freedom and Electronic Communications.”\(^{19}\) That report recommends that

a. Every college or university should make clear, to all computer users, any exceptions it deems necessary to impose upon the presumed privacy of communications, whether in print or in digital form.

\(^{17}\) For examples of procedural safeguards, see “Requesting Access to An Employee’s E-mail/Attachments or Computer Files | UCOP,” accessed March 15, 2013, http://www.ucop.edu/information-technology-services/services/ucop-it-services/accounts-e-mail-and-calendar/requesting-access-to-an-employees-e-mailattachments-or-computer-files.html.

\(^{18}\) The now-famous policy of the Harvard Faculty of Arts and Sciences may also offer a useful provision: “The faculty member is entitled to prior written notice that his or her records will be reviewed, unless circumstances make prior notification impossible, in which case the faculty member will be notified at the earliest possible opportunity.” Harvard University Information Security, FAS Policy Regarding the Privacy of Faculty Electronic Materials, http://www.security.harvard.edu/files/Security_Faculty%20Privacy%20Advisory%205.13.10.doc, accessed 14 March 2013.

b. There must be substantial and meaningful faculty involvement in the formulation of any such exceptions (e.g., requiring formal approval or endorsement by a faculty senate or comparable governance group).

c. The basic standard for e-mail privacy should be that which is assured to persons who send and receive sealed envelopes through the physical mail system—that envelopes would not be opened by university officials save for exigent conditions (e.g., leaking of a noxious chemical or ticking or other indicia of an explosive).

d. If a need arises to divert or intercept a private e-mail message to or from a faculty member, both the sender and the recipient should be notified in ample time for them to pursue protective measures—save in the rare case where any such delay would create imminent risk to human safety or university property.

e. The contents of any such messages that have been diverted or intercepted may not be used or disseminated more widely than the basis for such exceptional action may warrant.

f. Should the occasion ever arise to suspend or terminate an individual faculty member’s access to the computer system, so drastic a step should be taken only in response to a serious threat to the system, and should be preceded by a hearing before a faculty committee on the specific charge or charges of misuse or abuse.

g. Finally, similar safeguards should be fashioned (with full and meaningful faculty involvement in that process) and applied to other facets of electronic communications within the campus community—for example, the posting of sensitive evaluations or course materials, whose confidentiality may prove harder to maintain than might initially be supposed. Careful consideration should be given to privacy needs in myriad situations where unauthorized disclosure of electronic messages and materials could jeopardize personal reputations and other vital interests, and could ultimately deter free and open communications within the campus community.

These criteria should be incorporated to the extent they are consistent with Virginia law and policy.

4.1.2 The Office of University Counsel should specify procedures for monitoring electronic communications

In addition to a general policy, the university needs to develop specific procedures regarding the monitoring of electronic communications when necessary. With the implementation of the Office 365 system, requests for monitoring from any source will be sent to the Office of University Counsel, so it falls to that office to develop and post procedures for handling such requests. In developing these procedures, it is important to include, at a minimum, the following:

a. Specify what circumstances would prompt an e-mail search;

b. Describe the steps that will be taken upon the occurrence of the circumstances set forth in (a), and how the scope of the search will be determined;

c. Specify, by name and title, exactly who will have the user privileges to search other employees’ accounts.

d. Specify what records will be kept regarding any search that is undertaken. Such records should include which records were searched, when they were searched, who performed the search(es), and the circumstances—consistent with (a)—that prompted each search.
e. Clearly delineate what access other University personnel will have to the records referenced in part (d), including how University personnel may request access and how soon after making such a request they may expect to receive access.

f. Specify, by name and title, exactly who will be responsible for notifying users that their accounts will be searched and verifying that such notice actually occurs.

g. Specify, by name and title, exactly who will be responsible for providing timely responses to University personnel who properly request access to searched records and who will be responsible for verifying that such access is provided in a timely manner, as referenced in part (e).

4.1.3 The university should consider privacy interests as it revises policy 4011

As noted above, University Policy 4011 makes sweeping claims of university ownership of records produced by faculty and students. We have no doubt that this policy was created with good intentions, and we can imagine its importance for some purposes, especially when records might support a patent claim. However, we wonder if we need a policy so broad. We have not been able to find equivalent policies at the University of Virginia, Virginia Tech, or William & Mary, all of which presumably share Mason's interest in fostering sound recordkeeping.

As noted earlier, this policy was approved on 20 November 2008 and includes a provision that it will be reviewed every five years or sooner. As the university undertakes that review in coming months, it should consider the implications for e-mail and research privacy and adopt a policy that imposes the least possible burden on researchers consistent with the university’s obligations and interests.

4.1.4 The provost and deans should train promotion and tenure committees

Mr. Hunt explained that faculty who are denied tenure or promotion often submit FOIA requests for records concerning their cases. Mr. Moncure has explained that while departments may ask candidates for promotion to waive their rights to review records of their cases, there is no case law establishing the validity of such waivers. Thus, the provost and deans should ensure that department, college and university promotion and tenure committees are aware that their records may be viewed by the candidates whose cases they are deciding. Such guidance should be posted online, alongside existing information about promotion and tenure.

4.1.5 The university should consider alternative communications systems for human subjects research

Dr. Dade explained that other universities maintain systems for collecting survey data that are compliant with the Health Insurance Portability and Accountability Act (HIPAA) and more secure than such commercial systems as SurveyMonkey. She noted that such secure systems would be useful to researchers in health sciences, conflict zones, and other sensitive areas.

4.2 Freedom of Information Act policies

4.2.1 Mason should revise Policy 1117 (Responding to Virginia Freedom of Information Act (FOIA) requests for records) to codify the FOIA Compliance Officer’s actions in response to a FOIA request.

The current Policy 1117, last revised on September 30, 2011, has a brief “procedures” section requiring a department, school or activity receiving a FOIA request to transmit that request to the FOIA Compliance Officer. The policy is silent on what steps the FOIA Compliance Officer should take on receiving such a request.

The current FOIA Compliance Officer, Mr. Hunt, explained to the task force that on receiving a request, he contacts the person most likely to be in possession of relevant records, which is usually the creator of
the request. He relies on that person to make a good-faith effort to produce any responsive records and contacts another party, such as ITU, only if the person believes that it may possess responsive records that the creator does not have. Mr. Hunt also explained that if records meet the criteria for exclusion from FOIA, he will assert that exclusion.

These practices could go far to protect faculty and staff privacy within the scope of Virginia law, but they may need to be updated in response to new technical features, such as Office 365’s ability to preserve and search multiple accounts.

FOIA procedures should also be formally codified as policy. Such codification would enhance the transparency of the FOIA process, reassure faculty and staff that their privacy will be protected as much as possible, promote consistency in the actions of the various officials empowered to respond to FOIA requests, and ensure continuity as new people take on the duties of responding to FOIA requests.

4.2.2 The FOIA Compliance Officer should produce an annual report

By handling FOIA requests over several years, the compliance officer has gained a sense of what records are most likely to be the subject of future requests. For example, aggrieved students seek records about themselves prepared by their professors, faculty members denied tenure or promotion seek records concerning their cases, outside contractors want copies of awarded bids, and marketing or licensing firms want information about the athletic program. By compiling and posting an annual report of the number of requests received and the categories of records they seek, the compliance officer could alert faculty and staff to the kinds of records they might be expect to be subject to a future FOIA request, which could in turn help them be mindful when preparing and storing these records. Attention to FOIA cases at other Commonwealth universities and to university-related rulings of the Virginia Freedom of Information Advisory Council could be helpful as well.

4.2.3 The university counsel should defend assertions of exclusion

Again, we understand that FOIA provides records custodians the discretion to release even excluded records, and so the university cannot promise faculty and staff that it will not release excluded records in response to a FOIA request or defend assertions in court. However, Mr. Moncure has expressed his willingness to defend such assertions of exclusion, and we hope that he and his office will maintain this stance. We applaud the vigorous efforts of the University of Virginia counsel to secure “public university faculty in Virginia . . . a zone of privacy around their scholarly communications.”

4.3 E-mail policies

4.3.1 The university should explain how faculty and staff e-mail is stored

Mr. Sevon shared with us a document entitled “E-mail Retention for Mason Employees—Proposed,” explaining how faculty and staff e-mail will be stored in the new Office 365 system. This informative document should be posted publicly and updated as needed.

4.3.2 The university should establish separate e-mail accounts for student-employees

Students who work as research assistants, teaching assistants, or in other capacities should be given separate employee e-mail accounts to be used for correspondence relating to their duties as employees. This could protect their privacy as students and simplify matters should the university need to respond to a FOIA request or otherwise inspect their employee correspondence.

---

20 Respondents’ Joint Memorandum In Opposition to Petitioners’ Verified Petition for Mandamus and Injunctive Relief, American Tradition Institute v. University of Virginia, 24 July 2012.
4.3.3 The university should consider establishing separate e-mail accounts for faculty who serve in administrative roles

As noted above, the Public Records Act requires the university to preserve the correspondence of department and division heads for three years. It is to meet this requirement that the university plans to preserve copies of all incoming and outgoing faculty and salaried-staff e-mail for three years.

We believe that less drastic measures might meet the Public Records Act requirements. In particular, the university could establish separate, role-based accounts to be used by faculty in their administrative capacities. While such role-based e-mails do not appear to be common in American universities, some institutions have established them. For example, the Harvard case initially concerned a search of deans’ administrative accounts, not the separate, personal accounts that the university provides. And Mason already uses role-based accounts, such as support@gm.edu and webmaster@gm.edu, for various functions.

Activating three-year, “litigation hold” archiving for only specific administrative accounts would save tens of thousands of dollars each year. It would also give employees greater control over their communications, allowing them to delete at will messages that need not be preserved under the Public Records Act.

4.3.4 The university website should alert potential correspondents that their messages may be retained and shared

Some states with public records laws warn website visitors that the messages they send may become public records. For example, Florida requires its agencies to post “in a conspicuous location on its website” the warning that “Under Florida law, e-mail addresses are public records. If you do not want your e-mail address released in response to a public records request, do not send electronic mail to this entity. Instead, contact this office by phone or in writing.”

If Mason plans to store all incoming e-mail and to designate e-mail coming to department and division heads as public records, it should alert potential correspondents with comparable statements wherever e-mail addresses are displayed, including the People Finder and individual faculty and staff pages.

4.3.5 The university should consider appending information to outgoing e-mails

Below we suggest a disclaimer that individual faculty and staff may wish to append to their outgoing e-mail messages from Mason addresses. The university could make such a disclaimer the default for messages sent from the web interface, while giving faculty and staff the option to modify it as they wish.

4.3.6 The university should seek ways to inform faculty and staff about Virginia laws and policies and about their implications for the use of electronic communications

The task force suspects that many or most employees are not highly familiar with the requirements of Virginia policies about electronic communication, records retention, and FOIA requests. We suggest that the university identify opportunities to build awareness, such as orientation sessions for new faculty and graduate teaching and research assistants, and the renewal of computer passwords.

The university may also consider sponsoring one or more town hall meetings to discuss these issues.

---


22 Florida Statutes XXXIX 668.6076: Public records status of e-mail addresses; agency website notice
4.3.7 The university should consider delaying the implementation of the litigation-hold feature

While we understand the urgency of shifting to a new e-mail system, it is less obvious that the three-year litigation-hold feature need be activated at once. Postponing its activation for a few months would give faculty and staff time to prepare, e.g., by setting up new accounts for non-public business and directing correspondents to them.

4.4 Recommendations to department chairs

The task force believes that department chairs occupy a particularly important role in ensuring compliance with university policies and explaining to faculty their rights and responsibilities concerning records management and communication. The provost’s office may need to assist them with these tasks.

4.4.1 Department chairs should establish procedures for records management and communicate them with their faculty

The Library of Virginia’s Records Retention and Disposition Schedule General Schedule No. 111: All State Supported Colleges and Universities: College and University Records lists several categories of records that academic departments are expected to retain for certain lengths of time. Some of these records may be prepared by individual faculty yet retained by the department. For example, if a department collects syllabi from its faculty and then retains them, there would be no obligation for the individual faculty members under the schedule. Department chairs should explain which categories of records they will take responsibility for retaining and which, if any, remain the responsibility of individual faculty.

4.4.2 Department chairs should explain to promotion and tenure committees and to faculty their responsibility to preserve records and the limits of those records’ confidentiality

As noted above, faculty can and do submit FOIA requests for records of their tenure and promotion cases, especially when these cases are unsuccessful. Department chairs should alert committees, faculty members, and external reviewers that candidates may eventually see records of their cases.

5 Recommendations to individual faculty, staff, and student workers

5.1 Mason faculty and staff should use Mason e-mail accounts for transacting public business

Mason employees should use their Mason accounts for the transaction of public business. This clearly includes communications with students and communication with colleagues about the official business of the university, such as committee and administrative work. Public business, even if on private e-mail, is still subject to FOIA (§42.1-77), and individual employees are required to respond to FOIA requests.23

Though it is not forbidden by law for faculty and staff to forward mail from Mason accounts to non-Mason accounts for the transaction of public business, it is a bad idea, since it could lead to violations of FOIA and, for administrators and faculty acting in administrative capacity, the Public Records Act. Thus, faculty and staff should develop the habit of doing only university business on Mason e-mail.

It is acceptable for faculty and staff to use non-Mason systems for instant messaging, text messaging, and other non-e-mail text communication, that is not currently supported by Mason. So long as this instant correspondence is routine and administrative, it need not be preserved. If an action is taken or decision is made, employees should record that on an official medium, such as Mason e-mail; they can then delete the ephemeral messages. Employees should be aware that if their computer, phone, or other device, or their telecommunications provider, keeps a record of such messages, those messages may be subject to FOIA disclosure.

---

23 The statute obligates individual employees to respond to FOIA, and civil penalties up to $5,000 can be imposed for willful and knowing violations (§2.2-3714).
5.2 Mason faculty and staff should avoid using Mason e-mail accounts for personal correspondence

Employees are not forbidden from using Mason e-mail accounts and other electronic communications tools (such as Internet access, networked computers, voice-mail, cell phones, and smart phones) for personal use, so long as it does not interfere with their job performance or the operation of Commonwealth systems and networks. Moreover, the use of state resources does not make a record subject to FOIA if that record does not constitute the transaction of public business.

That said, state policy instructs that "Users should use their personal e-mail addresses and not those related to their positions with the Commonwealth when communicating or posting information for personal use." Similarly, the Virginia Freedom of Information Advisory Council recommends that "Public officials and employees should not commingle personal and official e-mails."

For purely personal communications—notes to family and friends, correspondence concerning one’s personal finances, hobbies, political and civic activities, etc.—this recommendation is fairly easy to follow. It is simple to set up a personal e-mail address, and many companies offer free accounts to those willing to view advertisements. We recommend that all faculty and staff take this step.

5.3 Mason faculty and staff should consider using alternative e-mail accounts for some professional and scholarly correspondence

A more challenging question is how faculty should communicate about their professional and scholarly activities. These activities may or may not constitute official duties and the transaction of public business. In the absence of settled law, we cannot offer clear criteria to distinguish between faculty activities that constitute the public business of the university and those activities that do not. The use of significant funds or resources provided by or administered by the university does create a greater likelihood that the activities should be considered public business, but even here, distinctions can be difficult. For example, if an assistant professor receives a study leave to revise his or her dissertation work for publication, the work done prior to the professor’s arrival at Mason would probably not become retroactively public. All faculty must use their discretion to make this distinction, and find rules that make sense for their own particular circumstances.

We asked the university counsel, the university FOIA compliance officer, and the university records officer about the consequences of faculty using their Mason e-mail accounts solely for communications that clearly constitute the transaction of public business—such as communication with students and communication concerning university governance—while using separate accounts for communication about their research, membership in professional organizations, and other scholarly pursuits. All agreed that establishing non-Mason accounts for these latter purposes could promote privacy. As the university counsel explained, if faculty use university letterhead and a university e-mail account, it is harder to assert that the records are non-public. Conversely, faculty and staff can signal that a record is not public by using non-Mason e-mail, maintaining separate computer folders, or marking certain records as personal and confidential.

Thus, faculty and staff concerned about the privacy of non-official professional correspondence may want to maintain at least three e-mail accounts: a Mason account for official business, a second, non-Mason

---

28 "Top 16 Free E-mail Services," About.com E-mail, accessed February 1, 2013, http://e-mail.about.com/od/freeemailreviews/tp/free_e-mail.htm. Services such as...
account for professional communication that does not constitute the public business of the university, and a third, non-Mason account for purely personal matters.

5.4 Faculty and staff could consider using signature files to remind themselves and alert correspondents to confidentiality limits

E-mail applications allow senders to append boilerplate text to the bottom of each outgoing message. Faculty and staff can use this feature to remind recipients of the provisions of Virginia laws and policies. For example:

Notice: The Commonwealth of Virginia claims the right to monitor messages sent to and from this address at any time, without notice, and without my permission. In addition, messages sent to and from this address may be subject to disclosure under the Virginia Freedom of Information Act.

This disclaimer may remind both the sender and recipient of the provisions of Virginia Department of Human Resource Management Policy 1.75 and FOIA, and help them use the account appropriately. Its language is stark, and faculty and staff must consider the tone such a reminder could convey.

Conversely, signature files appended to each outgoing e-mail from a non-Mason account could explain to correspondents that these addresses should not be used for the transaction of public business. The Department of Human Resource Management recommends the disclaimer, “The views expressed on this (website, blog, social media site) are my own and do not reflect the views of my employer or of the Commonwealth of Virginia.”

5.5 Researchers who collect sensitive information about human subjects should consider alternatives to e-mail

While we expect the Office of University Counsel to be diligent in avoiding the inappropriate disclosure of information about participants in research, it may be difficult to redact such information when preparing to disclose Mason e-mail in response to a FOIA request or subpoena. Researchers may wish to consider using alternative methods to communicate with participants in their research and consulting the Office of Research Integrity & Assurance.

5.6 Faculty and staff should act professionally in all their professional activities

There is always some chance that a written record intended to be private will become public, whether in accordance with established procedure or through mishap. We concur with the recommendation of the university’s FOIA compliance officer that Mason faculty and staff should be professional enough in their correspondence that they would be comfortable following any statement with the phrase, “your Honor.”

Respectfully submitted to the Faculty Senate, 3 April 2013

Zachary M. Schrag, Chair
Susan Brionez, Staff Senate
Tamara A. Maddox
Claudia A. Rector, ex-officio, Provost’s Office
Priscilla M. Regan
Stanley Zoltek, Faculty Senate

---

20 Virginia Department of Human Resource Management, “Policy 1.75, ‘Use of Electronic Communications and Social Media’.”