Minutes*

Academic Freedom and Tenure Committee
Friday, April 1, 2011
10:00 – 11:30
238A Morrill Hall

Present: Barbara Elliott, Karen Miksch (co-chairs), Tracey Anderson, William Craig, Joseph Gaugler, Linda McLoon, Christine Marran, Gary Peter, Terry Simon

Absent: None counted for a meeting called on short notice

Guests: Ken Hanna (Office of Information Technology), Tracy Smith (Office of the General Counsel)

[In these minutes: (1) emails and Minnesota Data Practices Act requests; (2) policy on non-renewal of P&A staff]

1. Emails and Minnesota Data Practices Act/Freedom of Information Act Requests

Professor Elliott convened the meeting at 10:00 and welcomed Mr. Hanna and Ms. Smith to discuss issues of concern as a result of the reports about the requests in Wisconsin and Michigan for copies of faculty members' email messages. She said they were invited to educate the Committee about Minnesota law, given the events that have been unfolding elsewhere with respect to requests for faculty emails.

Ms. Smith told the Committee that she is Associate General Counsel in the Office of the General Counsel who deals with the Minnesota Data Practices Act (DPA); Mr. Hanna explained he is Director of Security Assurance in the Office of Information and was representing Vice President Cawley, who was unable to attend.

Ms. Smith provided copies of "Public Records: Guidelines for Email," prepared by the University's Office of Records and Information Management in January, 2011, and "Guidelines for Use of Smart Phones for University Business," prepared by the same office in March, 2011. Both are appended to these minutes. Ms. Smith pointed out immediately, however, that the medium does not matter; these documents just happen to be for email and cell phones. State laws vary; the one here is the Minnesota Government Data Practices Act, which provides that government data are public unless another provision in the law says they are not; the presumption is that government data are public. The medium does not matter—it can be a text message, an email message, databases, etc. Nor does the system used matter (University or home computer); there are rules about work done on one's own computer and one cannot avoid the Data Practices Act by working on your own computer or your own email account. If the message or work is related to one's University work, it is government data.

One gloss on the law from the Minnesota Commissioner of Administration, who has the authority to issue advisory opinions about the law, is that if an organization permits personal use of work

* These minutes reflect discussion and debate at a meeting of a committee of the University of Minnesota Senate; none of the comments, conclusions, or actions reported in these minutes represents the views of, nor are they binding on, the Senate, the Administration, or the Board of Regents.

computers, personal messages are not “government data,” and they are not even covered by the Data Practices Act (and therefore need not be produced in response to a request under the DPA). University policy does allow personal use. So personal messages are not "government data," but work-related messages are "government data." If a message is work-related, and therefore "government data," it is public unless there is a provision of law making it non-public (or "private").

So if they receive a request for data, Ms. Smith related, they must first figure out what is "government data"—i.e., work-related—and what is personal and therefore not "government data." Then, after identifying the "government data," the next step is determining whether there is any provision of law making the government data "private." Emails with a student evaluating the student's work would be government data, but would be private government data, as would evaluations of an employee—those are protected under the provisions of FERPA and the DPA.

Ms. Smith provided an example. The University was asked for all text messages of a head coach. The coach had about 6000 text message on his University-supplied cell phone, some of which were work-related. So they downloaded all 6000 messages and, through a tedious and very long process, eliminated all personal messages, leaving only work-related "government data." Then, they evaluated the work-related messages to remove or redact data that the law deems "private." After removing private data (e.g., about particular students and job applicants), they ended up with a subset of the messages that were work-related and had to be released. Such requests are made occasionally, she said, and noted "Troubled Waters" and other incidents that have provoked requests; they usually focus on a specific employee or a certain period of time. In each case, they do the same analysis of emails before they are released. That is the way the law works.

There is no solid line that indicates when something will not be released, Ms. Smith explained. It depends on the context: What is the person’s job? Who was the email to? What were the contents of the email? If someone in her office sends a message to a spouse discussing the governor, that is personal. If a University vice president sends an email to another University official about the governor in advance of budget hearings, that might be work-related and therefore government data. It depends on what one's work is and to whom the message was sent, and conclusions require a contextual analysis. Many messages to students are work-related but if the messages involve personal student information or assessment they are "private" and will not be released.

Ms. Smith suggested that important material to keep is usually not kept in emails or texts messages, which tend to be transitory, therefore deleting email is a good option. Those media should not be used to communicate records that one (or the University) wishes to keep (e.g., notices of hearing, employee evaluations, etc.). Everyone can delete messages that do not set policy or take action, and deleting as one goes is the best practice. One should also then delete the deleted messages. The messages are then deleted forever as far as a DPA request is concerned. They will not go to unreasonable expense to try to recover emails from backup tapes that are meant for disaster recovery—it is technically too difficult. If messages are deleted, the General Counsel's office will not ask the Office of Information Technology to use advanced forensics techniques to try to retrieve them, nor do they believe that the law requires that be done, because it is virtually impossible to recreate targeted emails from such backup tapes.

There are faculty members who have been more frequently the target of DPA requests because of the nature of their work, Ms. Smith said. Interest groups may ask for information. The General Counsel's

office is aggressive in protecting faculty publications, research, and intellectual property, and can use the "trade secrets" provision of the law to protect research rights and the ability of a faculty member to publish. Beyond that, however, there is a great deal of data on the grants the University receives, expenses, and so on. There are rare occasions when a faculty member must deal with the hassle of a DPA request, and the University is not permitted to ask why the request is being made. The data practices law prohibits doing so.

Mr. Hanna told the Committee that he is involved in the technical side of the issue. In the University environment it is difficult to make broad statements because there are a lot of systems, people do things differently, and the institution is in the transition to Google. In general for deleted email, "if you can't see it, you can assume we don't go to forensics to recreate it" unless they are directed to do so by legal counsel. People should be mindful of what they need to keep and how long they keep it. One idea might be to print out those few things that might be official—which seems rather retro in this age—because it is easier to print the exceptions in one's email and then delete the rest. People should think about what they will keep so if they receive a DPA request, there will be fewer emails to go through, Mr. Hanna said. "You will probably not use all those old emails and you won't need to go through them." People at the University need to be aware of the Minnesota DPA, aware that they are public employees, and that they are subject to the law. Most of the trouble with a DPA request is the hassle factor, Mr. Hanna observed; they are tremendously time-consuming to respond to—and they never come at a good time.

Mr. Hanna said he would advise everyone, with respect to Google Gmail, to be mindful of the "All Mail" folder. Even if one deletes personal messages from a subfolder, they may still be in the "All Mail" folder.

In his unit, when there is a request for emails, the first thing they do is seek the guidance of Ms. Smith, Mr. Hanna related. Very few faculty members are subjected to DPA requests, but they have seen requests from ex-spouses, ex-girlfriends, and relatives of the deceased. They always obtain the opinion of the Office of the General Counsel about what they should do. They bend over backwards with faculty and staff—religiously—to try to ensure the privacy of email as best they can, Mr. Hanna assured the Committee, but they do have to obey the law. Mr. Hanna emphasized that the Office of Information Technology would never do anything on its own in response to a DPA request for emails without involvement of the Office of the General Counsel.

Ms. Smith said that Mr. Hanna raised a point worth noting. When they receive a DPA request, they do not treat emails differently from a filing cabinet: They work with the person who has the data to locate and produce responsive records. They do not enter into the person’s email or office to look for responsive records. They would only enter the email account of a faculty or staff member without the person's consent because they had received a subpoena or they were conducting an investigation of a violation of the law or of University policy. Even then, Ms. Smith said, they try to do the searches with the employee to avoid unnecessary intrusions into privacy; they see themselves as working with colleagues. DPA requests must be targeted, and they work with the employee to find the materials that have been requested. They will not do searches on their own.

Dr. Craig asked how many requests they receive per year. Ms. Smith did not have the number but surmised that it is probably about 100. Many of them are made when the University does something

that is big in the news—hires a new president, hires a football coach, the "Troubled Waters" kinds of incidents. The *Minnesota Daily* occasionally makes requests.

Professor McLoon inquired about emails that are stored on backup servers and are retrievable, with some effort, even though they have been deleted from a person's email trash folder. If asked about them, how do they deal with it? She has had a computer crash and email messages that had previously been deleted were found. Mr. Hanna said it depends whether the messages are viewed online or downloaded. If one only looks at email online using a browser, there may be a temporary copy of a few messages in the browser cache file on the local computer. However, retrieving them is getting into that theoretical forensics realm. (It should be noted that the University licenses security software called R-Wipe that will securely wipe these and many other computer cache files to safeguard legally private data.) Other than the cache file issue, if email is only accessed online, then all the issues with email copies existing on the local desktop/laptop/smartphone—and possibly on a backup server—are largely avoided. If instead, email is downloaded to one's computer, there are many issues and complications that can arise. For that and other reasons, use of the online browser interface is highly recommended.

How long does the server retain items, Professor McLoon asked. And if one deletes messages, and deletes the deleted messages, are they gone? If they are deleted as intended, they are pretty much gone, Ms. Smith said. Mr. Hanna agreed. If one uses the online method to access email, if a message is deleted and the trash is emptied, it is gone.

Someone filing a DPA request can ask for whatever they wish, Ms. Smith said, but if it will cost the University $50,000 to recover an email, she said she does not believe that is required by the law. If there is a cc on one's computer, however, that is different.

Who decides what would be released, Professor McLoon asked. The Office of the General Counsel is charged with interpreting the law for the University, Ms. Smith said.

What about when a DPA request is really not for information but to harass someone. There have been efforts over the years, by agencies that are inundated with DPA requests by a particular requester (which must be responded to free of charge to the requester), to narrow the scope of the law. All of the efforts to limit access because of the motive of the requester have failed, and the law has been made more specific in prohibiting inquiring about the motive of the requester. The University must comply with a request regardless of the motive of the requester.

Is there a difference between public and private universities, Professor Marran asked? And is there a certain point at which the University will be receiving so little state money that it is no longer a public entity? Ms. Smith said the law defines the University as a state agency. The legislature can also make laws that apply to private entities (e.g., non-discrimination laws), but in any event the University is a state agency, and is defined as an arm of the state by the constitution, and it would be an arm of the state even if the University received only 1% of its funding from the state. And that status is good for the University in many respects. Private entities can refuse to respond to a DPA request because they are not covered by the law.

Dr. Peter asked about materials he posts as an instructor, such as readings, notes, his work product on PowerPoint slides, etc. Can someone request access to them in order to see how he is teaching a course? The materials are available to the students in the class, not to the public. It is work-related so it

is government data, Ms. Smith said, and publicly available unless it falls under the exceptions in the law (private student data, private employee data, trade secrets, or patient data). Do they receive such requests? They have not, Ms. Smith said. Most such requests are for syllabi in order to critique teaching, Professor Gaugler said.

The upshot, Professor Gaugler concluded, is that if something has anything to do with the University, anyone can have access to it. That is correct, Ms. Smith responded. If one is obligated to release information from a University account or a personal account that is work-related, does the person do it or does the General Counsel's office do it? They rely on the person to provide information from a personal email account, Ms. Smith said; the University would have no access to it. They must rely on people being honest and reporting data they have. So, Professor Miksch said, if someone receives a request, they are not on their own—the General Counsel's office will help. They will, Ms. Smith affirmed. It is a collaboration with colleagues.

Professor Miksch said the question that had been raised by a faculty member, about looking into University email accounts without the knowledge of the account owner, has been answered: It is very rare, and only in response to a subpoena or legal or policy violation. But there are concerns that this does happen; if a faculty or staff member is concerned that someone is looking at his or her email, where would they go?

They should send a message to abuse@umn.edu, Mr. Hanna said. That is how they collect information. If someone sends a concern, Mr. Hanna's office can look to see if someone's email account has been accessed. They might see access five times, for example, and would ask the person if he or she accessed the account five times. He said he imagined that at an institution this large, there has been access to someone's email somewhere, but in his view concerns are often more likely a matter of paranoia than an understanding of what really happens. They will respond if asked by someone about his or her account, however, to see if there has been any intrusion.

Professor Anderson said it sounds like there is great support for responding to a DPA request. What channel do people use if on another campus? There are two ways, Mr. Hanna said. The most direct would be to contact Susan McKinney in the General Counsel's office; she is the coordinator of the Office of Records and Information Management. Or one can send a message to abuse@umn.edu, and they would forward the message to the General Counsel's office. Ms. Smith affirmed that they work with the coordinate campuses all the time. In responding to DPA requests, even if they are directed at the person whose emails are being sought, it is important that people go to the Office of the General Counsel, Mr. Hanna emphasized, and not respond alone.

Professor Elliott asked where, in all the conversation about the events in Wisconsin, the First Amendment and academic freedom stand. Ms. Smith said that the First Amendment protects employees in expressing themselves, and academic freedom in the University's policy goes beyond the First Amendment. The First Amendment protects employees against action taken against them by their employing institution because of their expression of views—they cannot be disciplined or suspended by the employer. That is wholly different from the public asking to see what views you expressed. The employer has no more or less ground to act just because someone requests emails or the like. The First Amendment governs relationships between the employer and the employee, not the public's right to information.

Professor Anderson said the Regents' policy on Academic Freedom and Responsibility talks about speaking as a private citizen, so could there be protection from some requests? There could be, Ms. Smith said, because the expression might be a purely personal point of view. It depends on the relationship of the statement to one's work. A personal expression of views would not be government data. So the public opinion piece of speech is protected while work-related expression is not, Professor Elliott concluded.

All of this suggests that education of faculty and staff about what can be available is needed, Professor Gaugler said. And people should know that if they make comments on politically-charged issues, they may be on the receiving end of a DPA request.

Professor Miksch said that she does not put in writing what she would not say in public, but the critics of the requests being made for faculty members' emails bring up the chilling effects such requests can have. Even though these are political beliefs covered by academic freedom, requests for emails might inhibit people from getting involved in public events by sending emails to their parents or sending petitions to colleagues. And those messages can be forwarded to others, Professor Gaugler observed—one does not know where they will go. (It was recalled during the discussion that a former chair of the Faculty Consultative Committee once commented that one should not put anything in an email that one is not prepared to see on the front page of The New York Times the next day.)

Professor Anderson asked if the law covered messages received as well as those sent. It also covers messages received, Ms. Smith said, if the messages are related to one's work.

Ms. Smith said that this is a very large institution with an enormous amount of government data (as defined by the law), but it receives only a small number of requests, and they cannot monitor all the University's activities because of a fear of a DPA request.

Professor Gaugler said that with respect to enhanced education for faculty and staff, it should include social media such as Facebook. One could put a comment on a Facebook page that would be sought as well. Ms. Smith said she thought it unlikely there would be a request for something written about the University on Facebook. The requests are related to work, not badmouthing a colleague on Facebook, for example—but, she added, she could not guarantee that a request could not include information on Facebook.

Professor McLoon asked if the guidelines that Ms. Smith had distributed had been provided to all faculty and staff at the University. They have not, Ms. Smith said. The guidelines can be found at http://www.policy.umn.edu/Policies/it/Use/ITRESOURCES.html#700. Professor Miksch said the University of Minnesota policy lets employees use their email for personal purposes, and that is why the personal messages can be redacted. Ms. Smith noted that Wisconsin does not permit such use, so the situation there is different.

Professor Marran asked if the University would help a faculty member who wanted to request information of a party outside the University. If someone wishes to make a request of the federal government related to one's work, Ms. Smith said, they would advise how to do so. If, however, the object of the request were, for example, a political party, such a request could be ignored because private organizations are not subject to a DPA request.

A related question from the Committee, Professor Elliott said, is about a sick faculty member—so sick he or she cannot communicate or do email. What happens when no one has the password to the computer? Is there a place or way that all should be informed about a safety net in that instance? In extraordinary cases, Mr. Hanna said, one can send a note to abuse@umn.edu and they will talk with the General Counsel's office to figure out what is appropriate. If one is incapacitated and the department or colleagues worry about missing deadlines, issues related to a grant, and so on, Ms. Smith said, they will first put out an email to stop communication to the incapacitated person's email account and will try to guard the person's privacy and review messages in a targeted way.

Professor Marran asked if there is a way to question the legality of a request. There is not, Ms. Smith said. What about requests that are fishing expeditions, Professor Marran asked? They must be reasonable, Professor Miksch said; someone may not ask for every email sent at the University. Ms. Smith said that they work with requesters so the University can respond in a reasonable way to help the requesters target what they really want, and if the request is so large, they have to work week by week. Sometimes the requester gets tired out. Is it possible to question the reasonableness of the request, Professor Marran asked? It is not, Ms. Smith said, it is the reasonableness of the time it would take the University to respond. Someone can ask for a work record, by topic or timeframe, for example, but even then it can be extremely time-consuming to respond—but the measure is not the time it takes to respond. What about a request for all emails from a faculty member that include, for example, the word "Muslim" in them, Professor Marran asked? How would that request be handled? They would need to review them and remove personal messages and determine which were work-related, Ms. Smith said. They would have to do the analysis and probably could not claim the request was unreasonable. Course materials from a religious-studies course could be requested, Professor Marran asked? They could, Ms. Smith said. And the General Counsel's office would have no control over such a request? They would not, Ms. Smith said. One must be prepared to receive such a request, Professor Gaugler said, and one's materials can be used and sliced and diced or put on a blog in a way that one cannot control.

Professor Marran asked if were possible for University policy, because of academic freedom, to filter requests and deny some of them. Professor Miksch reminded her that the motive of the requester does not appear to matter. So there is no way, by policy, to avoid the chilling effect of such requests, or to deem the request too broad or expansive or harassing, Professor Marran asked? Can the University make the requests more defined? The University cannot change the law by its own policy, Ms. Smith said; they can only work within the law. The sheer size of a request does not necessarily make it out of bounds. For example, data practices requests in connection with the academic fraud scandal on the men's basketball team in the '90s resulted in a roomful of data and took an enormous amount of time to produce—but most people would probably say there was a legitimate public interest in the issue.

Dr. Peter commented that in his course, he talks a lot about the Supreme Court, and posted an article about Justice Scalia receiving a traffic ticket. Someone could claim that the instructor was critical of the Supreme Court, but he can't control how other people use material. There are websites that monitor that kind of thing all the time, Professor Gaugler observed. Dr. Peter said there is a chilling effect because it makes him think about what he should use and it can affect his teaching. There is academic freedom but the intent of the law is to provide more disclosure, not less.

Many faculty members may not realize that even if they use non-University email, if the content is work-related, it can still be requested, Professor Marran said. Professor McLoon suggested the Committee make a statement because a lot of people are nervous and many feel vulnerable or potentially

vulnerable. And the Committee can make a statement to the Senate, Professor Elliott said—and it may also wish to send an all-faculty email, she added. This matter was brought up at the Senate meeting yesterday, and Professor VandenBosch reported that this Committee would be taking it up.

Professor Elliott thanked Mr. Hanna and Ms. Smith for joining the meeting. The Committee subsequently agreed it would like to revisit some of these issues at its meeting next week.

2. Policy on Non-Renewal of Academic Professionals and Administrators

Professor Miksch reported that the Committee on Faculty Affairs (SCFA) has begun reviewing proposed changes in the policy on non-renewal for P&A staff, but ran out of time so will return to it at its next meeting. There are two aspects of the changes in which she thought this Committee might be interested, given that non-renewal of P&A staff need not have a cause.

The existing policy provides that if a P&A staff member has been at the University for eleven or more years in a continuous appointment, the person received 12 months notice (and a sliding scale of notice for those who have been at the University for fewer years). The new proposal calls for six months' notice for those with eleven or more years of continuous employment. In addition, the existing policy extends the same notice provisions to P&A staff who have part-time appointments; the proposed revision provides two weeks' notice for anyone on a part-time appointment. SCFA will talk more about the policy and the Council of Academic Professionals and Administrators will make a statement about it as well.

Her concern, Professor Miksch said, is that people on annual appointments may already be reticent to speak (that is, exercise their academic freedom), even though they are covered by the Regents' policy on Academic Freedom and Responsibility, when non-renewal does not require a reason. To make the notice period even shorter can exacerbate that reticence. There is also a problem in that the proposed changes are to be retroactive. It seems inhumane to put people in that kind of position, Professor Marran commented.

The Committee agreed it would take up the issue at its meeting on April 8. Professor Elliott adjourned the meeting at 11:30.

-- Gary Engstrand

University of Minnesota

* * *

Public Records: Guidelines for Email
Office of Records and Information Management
January 3, 2011

Public employees should understand that any records they create related to University business—including text messages, voicemail messages, emails, and other electronic communications—are University records. These records therefore (1) should be managed according to University records

retention policies, and (2) may be subject to disclosure under the Minnesota Government Data Practices Act.

- **Remember, most of our work is public and is available to anyone upon request.** All University records, including emails, are public unless they contain information that is made private by the law. Examples of private information include private student and private personnel data. Much of our work does not involve private data, and must be produced publicly if requested.

- **The subjects of data almost always have the right to see the data.** With few exceptions, everyone has the right to the data that Minnesota governmental entities maintain about them. For the University, this includes our students and employees.

- **It is important to maintain professionalism in all communications, including emails.** Emails should be written with the same degree of professionalism as other University records. Individuals who are the subject of emails, as well as the public in many cases, have access rights to emails upon request.

- **Ownership of the computer system does not matter.** The Minnesota Government Data Practices Act governs all records relating to University business, whether those records exist on your work computer, your home computer, your smartphone, your University email account, or your private email account. By the same token, your personal, non-work-related emails are not government data subject to the law, even if they are on a University of Minnesota account. University business—especially when it involves private data—should be maintained on University of Minnesota systems.

- **Keep what you need; delete what you don't.** Emails tend to pile up, which makes it harder and more time-consuming to find what we need and to respond to requests for information. Much email consists of transitory, routine messages that do not need to be maintained. Delete what you do not need. Keep those emails that you need to keep for administrative purposes to document the work of your unit.

Examples of email that should be deleted once administrative use is completed:

- Transitory or routine messages that do not make policy or contain significant information.
- Telephone messages, either transcribed or downloaded through Gopher messaging
- Interoffice or interdepartmental communications that do not result in the formulation of policies
- Copied or duplicate messages sent as information only.
- Meeting notices
- Information request records that do not result in the formulation of policies.
- Routine announcements or information such as notices of meetings, queries regarding processes or ideas, general information, and electronic journals or listservs.

Examples of email that should be saved through the retention period:

- Email that sets or communicates policy or procedure

- Email that communicates who, what, why, when, where and how a transaction or decision was made.
- Email that documents or monitors student behavior, consultation or progress
- Email that documents personnel or employment decisions
- Email that documents or monitors personnel behavior, consultation or progress
- Email that documents changes in terms or conditions of contracts, grants, projects or services.

* * *

GUIDELINES FOR USE OF SMART PHONES
FOR UNIVERSITY BUSINESS
Office of Records and Information Management
March 2011

Public employees should understand that any records they create related to University business—including text messages, voicemail messages, emails, and other electronic communications—are University records. These records therefore (1) should be managed according to University records retention policies, and (2) may be subject to disclosure under the Minnesota Government Data Practices Act if someone requests them. These guidelines are intended to help you manage the business-related messages you send or receive on smart phones or similar devices (iPhone, iTouch, Blackberry, Trio, etc.), to appropriately keep what you should keep and to delete what is unnecessary.

The general rule is that business-related records that the University should retain must be kept on University—not personal—computer systems, and business-related records that do *not* require retention should be deleted as you go. This rule applies to University-related information transmitted on your smart phone or similar device by email, instant message, or text message, whether the phone is owned by the employee or provided by the University.

Text Messages

- Use text messaging only for **routine or transitory messages** that don't need to be retained by the University. Examples include notices of meetings, directions, and scheduling information, and other routine messages that you would not keep in a file if it were a paper communication. Don't use text messages to send policy, contract, personnel or student related University data.

- **Avoid sending private University data** in text messages. This includes student grade information, evaluative personnel information, etc.

- **Delete** your routine, transitory, business-related text messages as soon as possible.

- If for some reason, your text messages need to be saved under University retention policies, you must be able to **transfer messages to your unit's University network drive.**

- **Don't send social security numbers, passwords or credit card numbers** in text messages.

- **Don't text and drive** at the same time. This is a State of Minnesota law.

Voicemail

- Recordings of voicemail messages can also be considered government data under the Minnesota Government Data Practices Act. Follow the same principles for text messages—use voicemail with discretion; use it for routine, transitory messages that don't need to be retained; and delete as you go.

Email and Calendars

- **Password protect and auto-lock** your smart phone. No one should be able to pick up your smart phone and access your University email or your University calendar. The potential for disclosure of private data is too great.

Documents and Other Files on Your Smart Phone

- If your smart phone has other programs on it, such as Microsoft Office products, and you are using these programs for business-related purposes, **save those records to your network drive**—make sure they don't exist only on your smart phone.

- **Encrypt** any files that contain **private data.**

- **Delete files** from your device as soon as possible.

- Do not use personal or University provided devices to take, transmit, download, upload, print or copy **photos or videos** of University employees or students without their permission.