Frequently Asked Questions Attachment to Acceptable Use Rule

These frequently asked questions and their responses are provided as guidance for interpreting the Acceptable Use Rule and are not formally a part of the Rule itself. These questions and their responses may be modified or added to as this Rule is implemented over time as a result of new legislation or a change in the University culture.

1. Does using my personally owned mobile device on campus for non-university related personal business nonetheless trigger application of the Acceptable Use Rule if I use my personal device on the University's WiFi network?

   Yes. Once you connect your device to the University owned WiFi network, including U Connect and U Guest, your device becomes an IT Resource. The University does not monitor personal device use for content unless there is a reasonable suspicion of illegal activity.

   The definition of IT Resource is a Server, Workstation, Mobile Device, medical device, networking device, web camera or other monitoring device, or other device/resource that is a) owned by the University or used to conduct University business regardless of ownership; b) connected to the University's network; and/or c) that is creating, accessing, maintaining, or transmitting Information Assets and used for electronic storage, processing or transmitting of any data or information.

2. Does using TOR or otherwise masking my identity when transmitting an electronic communication over a University IT Resource violate the prohibition against "Forgery of Communications"?

   No.

3. What are some examples of where the notice provisions provided in the Rule need not be given because doing so will "seriously hamper the ability of the University to support its mission."

   Examples would include a User triggering a large denial of service of University resources, or a User generating a bomb threat email to the President. See also the provisions governing the giving of notice to a User found in the Acceptable Use Rule, section lll.D.2.b.

4. If I access my personal Gmail account on campus through the University's WiFi network and send a personal email unrelated to University business using my personal cell phone is the Acceptable Use Rule applicable?

   Yes. Once you connect your device to the University owned WiFi network, including U Connect and U Guest, your device becomes an IT Resource. The University does not monitor personal device use for content or access your personal email accounts

unless there is a reasonable suspicion of illegal activity. See also the provisions governing the giving of notice to a User found in the Acceptable Use Rule, section lll.D.2.b.

5. Under what circumstances may the University physically seize and access the contents of my personally owned laptop, cell phone or other mobile device?

   Under no circumstances may the University physically seize your personally owned devices.

6. Under what circumstances may the University access the contents of my University Box account?

   Because your Box account is a University resource, the circumstances under which the University may access the contents of your Box folders is under reasonable suspicion of illegal behavior and/or University regulation violations.

7. How does signature based detection or automated monitoring of email activity on campus work and what happens if such monitoring detects activity that violates the Acceptable Use Rule?

   These tools search for malware, and specifically defined unencrypted restricted data such as Protected Health Information (PHI). If there is a concern that a user's device is generating or enabling malware, the device may be taken off the network. If there is a concern that the user is misusing restricted data, the respective data owner will be contacted.

8. Who at the University is authorized to decide whether "reasonable suspicion of illegal behavior" exists? E.g. campus security? the University's Office of General Counsel? The University IT department? department chairs? Deans?, vice presidents? senior vice presidents? the president?

   Reasonable suspicion is a legal term used to describe a set of circumstances that indicate the basis for taking some action in connection with an individual. In order to qualify as "reasonable", the suspicion must be tied to a particular employee rather than a group of employees, and the suspicion must be based on specific and articulable facts, along with rational inferences taken from those facts.

   Reasonable suspicion is determined by the relevant Data Steward and/or Human Resources, in consultation with University's Office of General Counsel. Any other University representative must work through these key stakeholders to determine reasonable suspicion.

9. The Rule allows reasonable and limited personal use of University IT Resources, but requires a disclaimer if IT Resources are used for political campaigning or for commercial purposes. What are some examples of political or commercial activity that would require a disclaimer? Must I include a disclaimer in every tweet I send on my personal Twitter account if it relates to politics or commercial activities?

   Political activity that would require a disclaimer includes endorsing a political candidate, but this is not intended to prevent anyone from expressing a political view.

   Commercial activity that would require a disclaimer includes promoting a personal business product for sale using a University resource, but this is not intended to prevent anyone from communicating personal items for sale.

   If your personal media postings may be interpreted as formally representing the University, you should provide a disclaimer on your personal social media accounts. If a reasonable viewer/reader would not consider your statement to be on behalf of the University, no disclaimer is required.

10. May I be compelled by the University to disclose my password or to otherwise grant access to my personal social media accounts?

    No. No one at the University is authorized to ask anyone for their username and password, even to University owned systems.

11. What is the University policy or practice with respect to responding to requests by third parties to gain access to IT Resources that are used by an individual employee?

    In a civil case where the University is not a named party, the University would require a subpoena or other court order. In a civil case where the University is a named party, the University would require a formal discovery request from an attorney of record in the case.

    In a criminal case, the University would require a search warrant, court order, or other legal mandate.

12. If the University, pursuant to the Rule, accesses my Umail account, Box account or any other IT Resource I may be using in the course of an investigation into suspected illegal behavior, are there any guidelines or procedures in place to limit the access to the scope of the investigation or otherwise protect my personal privacy?

    Generally speaking, the scope of the investigation must be related to the scope of originating suspicion.

    In section III.D.2.b of the Acceptable Use Rule, language is included regarding when notice will be given to the User when stored personal information and electronic communications may be accessed.

13. If I have a question about whether the Rule applies to a particular situation or contemplated action, is there someone from whom I may seek guidance as to the application of the Rule?

    Dan Bowden, Chief Information Security Officer.

14. Does a violation of a University policy, as opposed to a violation of local, state or federal law, fall within the definition of “Illegal Activities” as that phrase is used in the Rule?

    No.