

USE OF ELECTRONIC AND TELEPHONE EQUIPMENT

RAILS provides or contracts for the communication services and equipment necessary for the efficient conduct of business. All business equipment, electronic and telephone communications systems, and all communications and stored information transmitted, received, or contained in RAILS' information systems (on premises or cloud based) are RAILS' property and are to be used primarily for job-related purposes. To ensure the proper use of communications systems and business equipment, RAILS may monitor the use of these systems and equipment from time to time.

1. Excessive personal use of electronic systems and the distribution of personal messages by employees is prohibited. Personal software or messages shall not be installed or stored on RAILS electronic equipment unless approved by the IT department. Employee personal use of RAILS equipment for outside business ventures or personal financial gain is prohibited. Likewise, employees are prohibited from bringing unauthorized electronic communications equipment to work to use with RAILS-provided electronic communications equipment and/or from accessing RAILS' systems with their devices without explicit permission from the IT Department. Such prohibitions include but are not limited to any type of external computer drives (such as flash drives) to save information from computer drives, personal laptops, and other wireless communications devices. Using such unauthorized equipment with RAILS-provided electronic communications equipment and/or accessing RAILS' systems without permission is considered to be theft of RAILS' intellectual property. Employees who create a RAILS profile/email account on their personal device without permission (or who refuse to delete their RAILS profile/email on their personal device when asked to do so) will automatically have their device reset to factory default by RAILS. This setting will delete all RAILS information from their device, but and will also delete any and all personal information (including, but not limited to, apps, contacts, pictures, videos, etc.) as well.

2. RAILS will, or reserves the right to, monitor the use of electronic systems and to review or inspect all material stored therein. No communications are guaranteed to be private or confidential.

3. The use of personal passwords assigned to the employee on RAILS-provided platforms is not grounds for an employee to claim privacy rights in the electronic or communications systems. RAILS reserves the right to override personal individual passwords. Employees may be required to disclose passwords or codes to RAILS to allow access to the systems. Refusal to do so would constitute insubordination and could result in discipline, up to and including termination from employment.

4. RAILS' prohibition against sexual, racial, and other forms of harassment ~~are is~~ extended to include the use of electronic and telecommunications systems. Intimidating, harassing, vulgar, obscene, or threatening communications are strictly prohibited, as are sexually oriented messages or images and/or messages that otherwise interfere with the job performance of fellow coworkers. Employees who receive email or other information on their computers which they believe violate this policy should immediately report this activity to their supervisor.

5. Privileged or confidential material, such as, but not limited to, ~~trade secrets or~~ attorney client communications, should not be shared with nonessential parties by email, faxes, etc.

6. Employees should respect all copyright and other intellectual property laws. For RAILS' protection, as well as your own, it is critical that you show proper respect for all the laws governing copyright, fair use

Commented [AS1]: Add "on premises or cloud-based" ?

Commented [AS2]: Would it make sense to add something about using RAILS equipment for personal financial gain or non-RAILS employment?

Commented [MH3R2]: Adding "Employee personal use for outside business ventures or personal financial gain is prohibited."

Commented [AS4]: What counts as "personal software or messages"? Seems a little broad - would activities like logging in to browsers or websites with personal accounts be prohibited?

Commented [MH5]: Comment received that explicit is hard to define but open to reasons this needs to be retained.

Commented [AS6R5]: Removing it seems fine to me.

Commented [AS7]: Need more info about the purpose of this section, definition of "create," and whether this is needed. It doesn't align with employee use of personal cell phones to connect to RAILS email, calendar, Zoom accounts, etc.

Commented [MH8R7]: Removing

Commented [AS9]: "passwords assigned to individual employees" might be more clear if we're referring to RAILS-provided platforms.

of copyrighted material owned by others, trademarks, and other intellectual property, including RAILS' own copyrights, trademarks, and brands.

7. Employees must be aware that electronic messages that have been erased or deleted can be retrieved by IT experts and can be used against an employee or RAILS. Therefore, employees should use the electronic systems only in the appropriate manner. RAILS records are public information and subject to records retention laws and Freedom of Information Act requests.

~~8. Employees should exercise care so that no personal correspondence appears to be an official communication of RAILS. Personalized RAILS stationery and business cards may only be issued by RAILS. Employees may not use the RAILS' address for receiving personal mail or use RAILS stationery or postage for personal letters.~~

~~9. A violation of this policy can may result in discipline up to and including termination of employment.~~

9. When RAILS is made aware of illegal activities using RAILS equipment, RAILS will promptly report those activities to the proper authorities in accordance with the law.

Commented [AS10]: This seems like it should be higher on the list, but the position doesn't matter as much as including it in the document, so it's fine as is.

Commented [MH11]: There was a request that this information is irrelevant to the subject matter of this policy and should be included elsewhere. Still evaluating where this would go alternatively.

Commented [AS12R11]: Agreed - this seems more like a general conduct guideline

Commented [MH13]: Additional request that we add a statement about reporting illegal activities if discovered on RAILS equipment

Commented [AS14R13]: Agreed

Commented [AS15R13]: From Wes: Illegal activities using RAILS equipment/property may cause RAILS to incur some liability for the activity if not reported immediately upon discovery.