PROHIBITED APPS: APPENDIX

SUBJECT: Updated Guidance on Usage of Prohibited Apps and Websites
FROM: archnews@UGA.EDU
Wednesday, March 26, 2025

Please see the directive below issued by Chancellor Perdue to all USG presidents regarding additional prohibited apps and websites. Questions about implementation or application of these guidelines should be directed to the Office of Information Security via helpdesk@uga.edu.

As stewards of public trust and protectors of sensitive institutional data, we must remain vigilant in the face of rapidly evolving cybersecurity threats. In December 2022, we informed you of Governor Kemp's directive prohibiting the use of TikTok, WeChat, and Telegram on state-owned devices and networks due to growing concerns about data privacy and security.

In today's interconnected world, privacy concerns have become a global issue. Bad actors—including cybercriminals and foreign entities—regularly exploit digital vulnerabilities to breach networks, steal sensitive information, and undermine trust in public institutions. These risks are particularly serious in higher education, where we manage not only operational data but also the personal information of students, faculty, and staff. Robust security measures are essential to safeguard privacy and maintain the integrity of our systems.

As part of this continued effort, Governor Kemp's administration has updated the list of prohibited apps and websites. In addition to TikTok, WeChat, and Telegram, the following apps are now also disallowed from use on any state-owned and/or -issued devices, including mobile phones, laptops, and tablets:

1. RedNote (social media app)
2. DeepSeek (AI chatbot)
3. Webull (online stock trading)
4. Tiger Brokers (online stock trading)
5. Moomoo (investing app)
6. Lemon8 (social media app)

These applications, many of which originate from foreign companies with unclear data handling practices, pose unacceptable risks to our networks, systems, and institutional data. Their use is therefore prohibited on all USG-managed devices unless required for an authorized law enforcement or security purpose.

As before, this restriction does not apply to students, faculty, or staff using these applications on personal devices. However, employees must not use any of these apps on devices—personal or institutional—that are used to access sensitive or restricted USG data, including health records, financial data, or personally identifiable information.

Use of these apps is permitted on devices funded by institutional foundations, provided no sensitive or restricted information can be accessed from those devices.

Importantly, institutions are not required to implement technical controls such as firewall blocks to enforce these prohibitions. While vigilance is critical, broad network-level restrictions could interfere with the free flow of information essential to academic inquiry and would not align with the permitted use of these applications on personal or foundation-supported devices.

We will continue to monitor this issue in partnership with state technology officials and cybersecurity experts and will provide updates as needed. Thank you for your ongoing commitment to protecting the data entrusted to us.

###

Created and approved by management team: April 22, 2025