4-OP-H-14 Mobile Applications, Digital Services, University Social Media, and Mobile Messaging

Responsible Executive: Provost and Executive Vice President for Academic Affairs and Vice President for Finance and Administration

Approving Official: Provost and Executive Vice President for Academic Affairs and Vice President for Finance and Administration

Effective Date: August 24, 2020

Last Revision Date: September 2, 2018, Non-substantive Change, 8-24-2020, Revised XX-XX-2026

I. INTRODUCTION

1. The University uses a number of different digital methods to communicate with students, employees, and the public in addition to the official University emails, websites, portal, and student information systems. These methods may include, but are not limited to, official university mobile applications (apps), push notifications delivered through university mobile applications, text messages, social media, and other digital services. Information distributed through these methods may also be made available through other means, depending on the importance and/or timeliness of the information. Communications sent by the University through these methods do not absolve students or employees of the need to monitor the official FSU email, portal, and applications of record (e.g., student, HR and financials systems) with regard to their status with the University. These digital methods addressed below are generally used to offer additional access to communications provided from official university sources.

II. POLICY

A. Definitions

1. For the purpose of this policy the following definitions will apply.
   - "Mobile application" (AKA "app") is defined as pre-packaged software designed to run on a mobile device such as, but not limited to, tablets, smartphones, wearables, digital assistants, voice interfaces, etc. that are available through native software, commercial app stores, or by download from the University.
   - "Digital Service" is defined as any content, media, activity, or service provided by official university sources through a digital medium.

- "Push notification" is a function within an app that notifies the user of new events or messages both within the app and outside the app, utilizing the mobile device interfaces to communicate with the user.
- "Telemetry data" or "metadata" is defined as data collected as a result of normal usage, interaction with digital services, system diagnostics, and tailored user experiences associated with a mobile device. Examples of telemetry data may include date/time of last access, access to wireless networks, approximate location, etc.
- "Social media" is defined to include websites, digital services, and apps that allow users to interact, receive, and share digital content with other users, or engage in social networking.
- "Mobile Messaging", is a general reference that encompasses both SMS and MMS communications.
- Short Message Service, "SMS" or "text messaging" is defined as an electronic communication sent and received by a phone using cellular carrier technology.
- Multimedia Message Service, "MMS," is defined as an electronic communication that can transmit a combination of text, video, sound, and images to a wireless or cellular device.
- "Universal inclusion" is defined as technologies that are compliant with the Americans with Disabilities Act or provides individuals with additional accessibility features to access data and information.

B. **Audience**

1. This policy has university-wide application for students, employees, and the general public utilizing university digital resources or services, which may include prospective students and employees. This policy was adopted to provide reference, authorization, and procedural guidance to students and employees on the implementation and use of various electronic communication systems that are generally considered voluntary use or are not covered by official University website and email policies.

C. **Mobile Applications and Mobile Messaging**

1. Florida State University is continuously developing and expanding an array of mobile applications that may be used by the University to disseminate general information as well as information specific to the individual. By downloading and installing these individual applications the student or employee is agreeing to receive information and notifications via these apps.

a. The University may actively promote mobile apps to the student body, employees, and the public. Any digital services deemed "voluntary use" by the University will not require individuals to download specific applications as a requirement for participation in University services or activities, including, but not limited to, events, academic classes, or research, except in cases where activity is specific to mobile apps and/or devices and the use of the app is integral to the individual's participation.

b. Wherever possible official University apps must carry the University brand and follow the branding guidelines set forth by University Communications, to the greatest extent possible within the application design.
c. In general, the University provides user privacy and data safeguards as identified in the University Information Privacy Policy. Telemetry data collected through the use of apps or digital services may be reviewed for the purpose of verifying functionality of the app and/or improvement of functions and services. In select cases, where telemetry data may be used for purposes other than the above stated, individuals downloading the app must be presented with an informed consent notification and must positively indicate they accept the terms and conditions of the use of the application. Such terms and conditions must specify at a minimum, the type of data collected, purpose, and use of the data.
d. Individuals downloading apps consent and agree to pay any costs associated with data, text message, or SMS services used as part of these applications. This may include push notifications, location-based messages, etc.
e. Apps developed by the University, or provided by a third party with whom the University has contracted to develop such an app, will be configured by default to enable the minimum number of application functions required for essential operation of the app. All other functionality will be defaulted to a disabled setting with options available to users to enable functions as they choose. This includes defaulting all push notifications to "off" or its equivalent. Apps must be designed with user privacy in mind. For this reason, functions within the app should be limited to only those device options needed to interact with the app. Applications are required to request permission from a user for access to any mobile device services or user data, including location, microphone, contacts, calendar, email, etc. Applications must clearly state the purpose of the requested permission and must provide clear instruction on how to cancel or remove permissions for services which are approved by the user.
f. Mobile apps that represent university services or that communicate with the individual as a representative of the university must be sanctioned by the appropriate university organization or official. The responsible entity/entities that owns/administers the application is responsible for communicating changes, enhancements, or removal of functions or the app itself, including removing it from the respective app stores and issuing any cease and desist order that includes the marketing of the FSU affiliation.

2. It remains the application user's responsibility to take adequate and appropriate measures to safeguard their device(s), including University owned devices, and any personal data stored on the device. (See also **4-**

OP-H-12 Information Privacy Policy) In the event that a mobile device is compromised, lost, or stolen, it is the user's responsibility to report the incident to the police department and the appropriate wireless service provider.

3. Inappropriate mobile messages by students or employees may result in disciplinary review and sanctions under the appropriate code of conduct or disciplinary guidelines.
4. Message and push notifications to more than 500 individuals require approval by an individual at the Academic Dean of a college/school, Dean of Undergraduate Studies, or Vice President level or higher. Exceptions to this requirement are notifications that follow the established emergency notification procedures or notifications related to routine maintenance or updates to app features, function, or nature
5. Messaging to students will be limited to academic and administrative units within the University for the purpose of notifying students about core business and academic operation such as deadline reminders, advising, student account or financial aid information. Users may review additional notification messages for activities and events beyond these core business and academic operations where such options are provided.

D. **Social Media**

1. Academic units and administrative offices may utilize digital services to establish social media accounts in order to support and communicate official information to interested parties who may choose to subscribe to the service. Official social media sites or accounts that represent a specific office must restrict its messages to those appropriate and relevant to the domain or discipline area of the office. Official University accounts shall be consistent with the University's Branding Policy 2-8. (See also **Policy X-XX Social Media Policy**)
2. ~~Individuals who subscribe to one or more social media accounts related to the University do so with the understanding that information posted to the platforms by the University, or by the individuals themselves, may be available to the public. As a result, information shared in the public domain may be subject to the posting standards of the social media service. Inappropriate usage by students or employees on official University social media sites may result in a referral to the Dean of Students and/or the Office of Human Resources, as appropriate, for review and any appropriate action.~~

~~a. The University recognizes, embraces and supports the need and right of free speech in the public domain. In the event that an individual posts information that violates a state law, Federal law, or University policy, legal or disciplinary action may be brought against that individual, and the University may choose to remove the post and/or block the user to prevent additional violations. In cases where students or organizations establish their own social media sites and exchange information that is prohibited under the Student Conduct Code, Academic Honor Policy, and other applicable policies, sanctions may be brought against the individual or organization in question.~~

b. Employees, including faculty members, adjuncts and graduate assistants, who use social media in instruction of courses should refer to the University's 4-OP-H-12 Information Privacy Policy concerning the transfer of information classified as protected or private to social media sites.

3. Employees using social media, whether a University account or otherwise, should be aware of the following risks and responsibilities that exist when using these platforms:

a. Some information communicated using the University's network may be defined as a public record by Florida law and be subject to the provisions of Chapter 119, Florida Statutes.

b. The same University regulations and policies that generally govern behavior as a University employee also apply to activities online. This includes maintaining the confidentiality of University trade secrets, research and intellectual property, copyrighted material, and private or confidential information. Certain information is protected under state and/or federal law, including, but not limited to, limited access employee records pursuant to Section 1012.91, Florida Statutes, student information under the Family Educational Rights and Privacy Act (FERPA), and medical information pursuant to the Health Insurance Portability and Accountability Act (HIPAA). Attorney-client privileged information is also protected from disclosure.

c. Individuals may not represent themselves as a spokesperson for the University without explicit authorization from the appropriate university authority. Posting information online related to an individual's work as part of the university, or to subjects associated with the University, must clearly state that such statements are not made on behalf of the University. Any such statements should include a disclaimer, similar to the following: "The views and opinions expressed are strictly mine and in no way represent those of Florida State University, the Board of Trustees or the State of Florida."

d. Individuals should avoid using statements, photographs, video, or audio that reasonably could be viewed as malicious, obscene, defamatory, abusive, unlawful, threatening or intimidating, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts that may harm someone's reputation or that could contribute to a hostile work environment on the basis of any recognized protected group status.

4. Employees may be subject to disciplinary action if their actions on social media or other online activities violate University regulations or policies. Students may be subject to review under the Student Conduct Code and/or the Academic Honor Policy.

5. These policy guidelines shall not be construed or applied in a manner that improperly interferes with employees' rights under Chapter 447, Florida Statutes, and/or Section 7 of the National Labor Relations Act, nor shall

~~they be construed to interfere with a faculty member's academic freedom as defined in Article 5, Academic Freedom and Responsibility, of the FSU BOT – UFF Collective Bargaining Agreement.~~

E. **Mobile (Text) Messaging**

1. Students and employees who provide a phone number within their respective information systems may receive text notifications. By providing this number, the student and employee is opting-in to receive notifications from academic and administrative University offices.

1. Text notification numbers will automatically be added to the University emergency alert system. In the event a text notification number is updated, the emergency alert notification number will be updated as well. Removal of the number from the text notification will not automatically result in removal from the emergency alert system. This will require the employee or student to separately remove the number from the emergency alert system. The FSU Emergency Notification System will be used only to transmit notifications of conditions that threaten the health and safety of persons on campus. In addition, the University reserves the right to use text messages for surveys needed to support University operations in the event of emergencies.

2. Text messaging to students will be limited to academic and administrative units within the University for the purpose of notifying students about core business and academic operation such as deadline reminders, advising, student account, financial aid information, or to promote student success. Students that choose to opt-in for text messages with individual student organizations, clubs, groups, etc., do so at their own discretion. Text message numbers will not be provided or used for non-emergency surveys.
3. Student text notification and emergency text numbers are classified as FERPA protected data and are confidential under both federal and state law. In order to preserve this communication channel, academic and administrative offices are restricted from providing data sets of phone numbers to third-party entities that have no contractual connection to the University, including for the purpose of sending mass text messages to students. Academic and administrative offices may use a University-authorized tool such as a mobile app downloaded by the individual, enterprise CRM solutions, learning management system tools, or similar University-wide communication tool.
4. Inappropriate text messages by students or employees may result in disciplinary review and sanction under the appropriate code of conduct and/or policy.

III. **LEGAL SUPPORT, JUSTIFICATION, AND REVIEW OF THIS POLICY**

1. BOG Regulation 1.001, 1.001(3) (g), University Board of Trustees Powers and Duties, Delegations from Board of Trustees to President