CONTENT:

- Purpose
- Scope
- Policy
- Signature lines

PURPOSE:

The primary purpose for this document is to establish the basic guidelines for the use of Smart Device in the Division of Student Affairs.

SCOPE:

As technology continues to advance and the worlds that we each live in continue to be redefined, it is not a surprise that we find ourselves blending our work with our family and other business lives. We cannot and should not ignore the emergence of technologies that can be used to support all of our lives. This guideline attempts to take steps in combining the many lives that we live without the need to carry many devices.

POLICY:

As we acknowledge the statements above, I must also share a major concern that you and I should have relating to the blending of our lives, in particular, as they relate to our business life on our personal devices.

University Business Use

Student Affairs employees should understand that any records they create related to University business – including text messages, voicemail messages, emails, and other electronic communications are deemed to be institutional data records.

Records:

- Should be managed in accordance with the following University policies, Computer and Network security (AD20), Institutional Data (AD23), University Archives and Records Management (AD35).
- May be subject to disclosure under state acts if requested.

The following guidelines are intended to help staff in the Division of Student Affairs who have received permission from their departmental directors and their AVP or the VP to manage the business-related messages send or receive on smart phones or similar devices (iPhone, Blackberry, etc.).

The general rule for all business related records should be kept in an environment on your Student Affairs secure drives. However, there are times when you are away from the office
and have the need to remain connected for many reasons. The policies and guidelines identified in AD20, AD23 and AD35 also applies to smart phones and other smart devices and the information transmitted and received by email, instant message (IM), or text message, whether the phone is owned by the employee or provided by the University.

Miss-use of Smart Phones or Smart Devices
- It is never appropriate to use personal or University provided smart devices to take, transmit, download, upload, print or copy photos / videos of University employees or students without their permission.

Text Messaging Use:
- 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. Do not use text messages to send policy, contract, personnel or student related University data.
- Avoid sending private University data in text messages. This includes FERPA information, staff information relating to evaluations, etc.
- Delete your routine, business related text messages as soon as possible.
- If for any reason text messages must to be saved because of retention policies, you must transfer that message(s) to your secure Student Affairs network drive.
- PCI policies are in full force when using your smart phone or smart device. Do not transmit social security numbers, passwords or credit card numbers in text messages.
- Avoid texting while driving. This is a pending state law in Pennsylvania and is being enforced on many roads in the state.

Voicemail:
- Recordings of voicemail messages can also be considered University data. Follow the same principles described under text messages—use voicemail with discretion; use it for routine, transitory messages that do not need to be retained; and delete them often.

Email and Calendars
- If you are synchronizing and or receiving email over the air, the smart phone or smart device must be password protect and you must enable and auto-locking scheme on that device. No one should be able to pick up your smart phone and access your email or gain access to your Student Affairs or University information. The same potential for disclosure of private data is the same as that of a laptop or other devices.

Documents and Other Files on Your Smart Phone:
- If you are using other software which will allow you to house institutional data, such as MS Office products, you should save those documents on our SA secure server(s) if the data is for work purposes.
Lost Smart Phones and Devices:

- In the situation where a smart phone or smart device is stolen or lost, the situation will be treated as a potential compromise. The rules governing compromises will be followed including if necessary, the removal of the device for evaluation by ITS – Security Office. If this is a personal device, your personal data will be subject to review as well.

Future direction of Smart Devices and other Mobile Devices:

- Mobile device requirements will include an encryption clause and will require the device to be encrypted if it is used to conduct any University business. Individuals using personal devices will not be excluded from this mandate.

Created: December 17, 2009