GUIDELINES FOR SMART PHONES, TABLETS, AND SIMILAR DEVICES FOR UNIVERSITY BUSINESS

Office of Records and Information Management
Office of General Counsel
April 12, 2011

Public employees should understand that any records they create related to University business—including text messages, voicemail messages, emails, and other electronic communications—are University records. These records therefore (1) should be managed according to University records retention policies, and (2) may be subject to disclosure under the Minnesota Government Data Practices Act if someone requests them. These guidelines are intended to help you manage the business-related messages you send or receive on smart phones, tablets, or similar devices (iPhone, iPad, iPod Touch, Blackberry, Android, etc.), to appropriately keep what you should keep and to delete what is unnecessary.

The general rule is that business-related records that the University should retain must be kept on University—not personal—computer systems, and business-related records that do *not* require retention should be deleted as you go. This rule applies to University-related information transmitted on your smart phone or similar device by email, instant message, or text message, whether the device is owned by the employee or provided by the University.

Password Protect & Autolock Your Device

- No one should be able to pick up your device and access University data. The potential for disclosure of private data is too great.

Text Messages

- 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. Don't use text messages to send policy, contract, personnel or student related University data.

- **Avoid sending private University data** in text messages. This includes student grade information, evaluative personnel information, etc.

- **Delete** your routine, transitory, business-related text messages as soon as possible.

- If for some reason, your text messages need to be saved under University retention policies, you must be able to **transfer messages to your unit's University network drive.**

- **Don't send social security numbers, passwords or credit card numbers** in text messages.

- **Don't text and drive** at the same time. This is a State of Minnesota law.

Voicemail

- Recordings of voicemail messages can also be considered government data under the Minnesota Government Data Practices Act. Follow the same principles for text messages—use voicemail with discretion; use it for routine, transitory messages that don't need to be retained; and delete as you go.

Email and Calendars

- **Again, password protect and auto-lock** your device—it will protect the University data in your email and calendar.

Documents and Other Files on Your Device

- If your device has other programs on it, such as Microsoft Office products, and you are using these programs for business-related purposes, **save those records to your network drive**—make sure they don't exist only on your device.

- **Encrypt** any files that contain **private data.**

- **Delete files** from your device as soon as possible.

- Do not use personal or University-provided devices to take, transmit, download, upload, print or copy **photos or videos** of University employees or students without their permission.