

Lake Forest College Mobile Computing Device Policy

The following policy applies to the use of mobile computing devices. Examples of mobile computing devices include laptops, tablets, smart phones, and e-readers. The College's *Acceptable Use of Information Technology Resources at Lake Forest College* governs the use of any mobile device that is used on the College's network regardless of whether or not that device was purchased with College funds. The Acceptable Use Policy also applies to the use of a personally owned mobile device if Lake Forest College funds pay for part or all of the data plan for that device. In those cases, the policy applies no matter where the mobile device is used.

Mobile computing devices purchased with College funds remain the property of Lake Forest College. All mobile devices purchased with College funds should be reported to the Office of Library and Information Technology so they can be entered into the College's computer hardware inventory. Mobile devices purchased with College funds must be returned to LIT (or the appropriate academic department or administrative office) if the employee to whom the device was issued leaves the employment of the College.

LIT will be responsible for the maintenance of all mobile computing devices purchased with College funds. LIT staff will not visit homes or go to off-campus locations to support these devices.

Mobile devices purchased with College funds will be configured with a standard suite of software programs that are appropriate for the type of device and intended use. The College may provide other software based on the end user's professional needs or the requirements of the device. The software should be used in compliance with the College's Acceptable Use Policy. Individuals may not load software for personal use such as games, entertainment software, or personal finance software on a College-owned mobile device.

Sensitive information should not be saved on a mobile device without taking appropriate precautions. Sensitive information includes any data that is protected by College policy, or by local, state, or federal laws or regulations. This includes, but is not limited to, education records of students, and confidential internal College information.

Individuals who are issued mobile devices are responsible for maintaining an appropriate backup of the data files stored on the device, especially of work-related documents and files that cannot be retrieved by reinstalling the operating system or programs. Network storage is a good option for backing up work-related documents and files. LIT staff are available to assist with this process. For some especially large projects, network storage may not suffice. In such instances, the individual should consult with LIT to identify other appropriate means of storage and backup. Personal data and information should not be stored on the College's network storage.

Because of their portability, mobile devices are susceptible to theft. Individuals for whom a mobile device has been purchased are responsible for preventing damage to or loss/theft of the device and may be responsible for costs to repair or replace it if the damage or loss is due to negligence or intentional misconduct. Individuals may wish to consider purchasing insurance to cover accidental damage to a College owned mobile device.

The loss of any mobile device purchased with College funds must be reported to the Director of LIT immediately. Theft or loss that is known to have occurred on campus should also be reported to Public Safety. If the theft or loss is known to have occurred off campus, it should be reported to the appropriate police department and a copy of the police report should be provided to the Vice President for Business as soon as it is received from the police.

General Security Best Practices for Use of Mobile Devices

- Keep your mobile devices with you at all times or store them in a secured location when not in use. Do not leave your mobile devices unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.).
- Mobile devices should be password protected and auto lockout should be enabled. The password should block all access to the device until a valid password is entered. The password used should be as strong a password as your device will support.
- Enable a “remote wipe” feature if available. This also includes features that delete data stored on the mobile device if a password is not entered correctly after a certain number of specified tries.
- Do not circumvent security features or otherwise “jailbreak” your mobile device.
- Standard security protocols should be followed. This includes ensuring your device has current anti-virus software and all operating system and application updates and patches. Firewalls should be enabled if possible.
- Do not install software from unknown sources as they may include software harmful to your device. Research the software you intend to install to make sure it is legitimate. When in doubt, consult with LIT.
- When installing software, review the application permissions. Modern applications may share more information about you than you are comfortable with, including allowing for real time tracking of your location.
- Storing of personal data on a mobile device is risky. If you lose the device, you could lose your data.
- When using a mobile device to connect to a wireless network in a public area such as a coffee shop or hotel, use of the College’s VPN is encouraged to protect the security of information being transmitted.

Reviewed and endorsed by the LIT Advisory Committee 9/27/2012