Illinois Early Intervention Clearinghouse
University of Illinois at Urbana-Champaign
51 Gerty Drive, Champaign, IL 61820-7469
Toll-free: (877) 275-3227 Email: Illinois-eic@illinois.edu
http://eiclearinghouse.org

Please save this information.

EIC Technology Loan Program: Use and Responsibilities

By borrowing and accepting this equipment, you agree to the following responsibilities and conditions:

Care and Malfunction

You are responsible for the proper handling, storage, use, care, maintenance, and return of the device to the Early Intervention Clearinghouse. You will return the device to the Early Intervention Clearinghouse on or before the designated due date.

If the technology malfunctions, you will immediately contact the Early Intervention Clearinghouse at (877) 275-3227.

Loss and Liability

In the event you lose the device, you may be liable for its current replacement. You will immediately contact the Early Intervention Clearinghouse at (877) 275-3227.

You may be charged the full replacement fee if you do not return all of the technology you borrowed or if the technology is returned damaged. The potential costs to replace a damaged piece of technology are itemized below.

- iPad: Repair cost determined on a case-by-case basis; $600 for full replacement
- Hotspot: $50 for full replacement
- iPad cover: $20 for replacement
- AC adapter/power cord for iPad or Hotspot: $50 for replacement

Sharing and Theft

You will not share the technology with any third party.

In the event that the technology is stolen despite your efforts at safekeeping, you will report the theft to the local law enforcement agency and provide a copy of that report to the Early Intervention Clearinghouse to prevent any replacement fees from being assigned to you.

Unacceptable Use

The following activities are an unacceptable use of this technology and may be subject to legal implications:

- Copying or distributing any proprietary software or hardware loaned through the Early Intervention Clearinghouse.
- Violating the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way.
- Engaging in malicious activities.
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the networks or systems of any individual or entity.
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages.
- Sending, receiving, or accessing pornographic materials.

Use and Return of the Technology

You will not attempt to load or delete any apps or programs or attach any equipment not designed for use with the technology.

When technology is returned, all files (including pictures and videos), programs, and other data stored on the device will be deleted.

This iPad is supervised and managed by University of Illinois at Urbana-Champaign.

Device Supervision

Supervision gives institutions greater control over the iOS devices they own. With supervision, your administrator can apply extra restrictions like turning off AirDrop or preventing access to the App Store. It also provides additional device configurations and features such as silently updating apps or filtering web use.

See what your administrator is supervising

Your administrator controls settings on your device by installing profiles. If you want to see which features your administrator has modified, you will need to check your settings. Tap Settings > General > Profiles & Device Management. If there is a profile installed, tap on it to see which settings it modifies. To learn more about the features changed by your organization, ask your administrator.

Access to location and Internet activity

Your organization cannot access the location of your device without using a feature called Managed Lost Mode. When this mode is enabled, your device is first locked and only then can your device administrator see its location. If your administrator puts your device into Managed Lost Mode, you will see a message on the lock screen. If your organization has requested the location of your device , a notification will remain on the lock screen until the device is unlocked by you. Your organization can't see the location of your device without locking it and showing this notification to you.

Supervision can be used to configure your device to provide access to Wi-Fi networks, VPN servers, proxy servers, and Internet content filters. These network settings have the ability to route your Internet activity through your organization's networks where it can be secured and also possibly viewed by your administrator. To learn more about how your Internet activity is being used by your organization, ask your administrator.