Lower Columbia College
Mobile Device Guidelines

Purpose

These guidelines govern all use of mobile devices to accomplish Lower Columbia College's (LCC) mission. They also define the appropriate use and security configuration for personal devices which are granted access to Lower Columbia College's network and resources. For additional information, refer to the Washington State Office of the Chief Information Officer (OCIO) Policy No. 191 - Mobile Device Usage.

Scope

These guidelines apply to all individuals affiliated with LCC, including: employees, contractors, consultants, temporaries, work-study students, etc. They also apply to all personnel affiliated with third parties who use mobile devices which are capable of displaying or editing LCC's information.

Mobile Devices

Laptop Computer

- LCC-Owned laptops are supplied by IT Services and IT Services provides all primary technical support as needed.
- Personally-Owned laptops may be used in limited cases such as to access the public wireless network, web-based email, and LCC web applications. IT Services does not provide any support for personally-owned laptops.

Cellular Devices

- In general, these are devices which incur a monthly service charge for connectivity via a cellular carrier.
- LCC-Owned cellular devices are provided by IT Services. IT Services provides limited technical support for cellular devices.
- Personally-Owned cellular devices may be used in the same manner as personally-owned laptops. IT Services does not provide any support for personally-owned devices.

Non-Cellular Mobile Devices

- In general, devices which do not incur service charges for connectivity via a cellular carrier.
- Ownership and support is the same as for cellular devices described above.

LCC-Owned Devices

If using an LCC-owned device, IT Services will provide the necessary software and guidelines for maintaining and protecting data on the device. This may include restrictions on certain classes of data, apps, and other functional aspects of the device. These restrictions may limit use compared to the use of personally-owned devices.

- For any apps not specifically required to accomplish LCC's mission, an employee should seek approval from his or her supervisor and IT Services before downloading.
- IT Services retains the ability to "re-image" or "wipe" the device which erases all apps and data by resetting the device to its original default configuration.

- End users are responsible for backing up any data stored locally on the mobile device.
- Managers and supervisors are responsible for all mobile devices assigned or deployed to employees in the department which they supervise.

Security

Each employee is accountable and responsible for protecting LCC's intellectual property, including employee and student information. All users must take reasonable steps to protect the mobile device against loss or theft and to prevent unauthorized access to, or use, disclosure, or acquisition of, LCC information stored on the device.

The device must meet minimum security requirements. Employees should use a method such as a swipe pattern, fingerprint ID, or passkey (4 digits minimum) for locking the device.

LCC reserves the right to prevent access by any mobile device running applications that IT Services believes poses a risk to its network infrastructure. IT Services may limit the participation of any device that is "jailbroken or rooted," i.e., the use of software to "free" the device from limitations present at the time of purchase by the manufacturer or the telecommunications carrier.

Remote Data Wipe

Protecting LCC's intellectual property and the personal information of the college's employees and students is the college's primary concern. As such, IT Services reserves the right to remotely wipe apps and data from any mobile device that is connected to LCC's systems. There are two methods for IT Services to remotely wipe a device.

1. Account Wipe: An Account Wipe will only remove LCC apps and LCC data, including email, calendar items, contacts, applications and documents that are stored on the device. Personal apps and data will remain intact. An Account Wipe feature is not supported by all Mobile Device Management (MDM) solutions.

   IT Services may initiate an Account Wipe in the following circumstances:
   a. Upon an employee's separation of employment from LCC
   b. Upon notification that the device is lost or stolen
   c. When LCC has reason to believe that the information is being, or may be, at risk of misappropriation or other misuse.

2. Device Wipe: A device wipe will reset the device back to its default settings (all data will be deleted). A Device Wipe is immediate and irreversible. Any data or information that has not been previously backed-up or synchronized will be lost. This includes photos, music, applications, emails, text messages, videos, and any other content on the device.

   IT Services may initiate a Device Wipe on an LCC-owned device in the following circumstances:
   a. To provide service or support such as upgrading the operating system, preparing for a new quarter, or re-deploying the device to another department or employee
   b. Upon notification that the device is lost or stolen

c. When LCC has reason to believe that the information is being, or may be, at risk of misappropriation or other misuse.

LCC will not be held responsible for the loss of any personal data stored on the device. Further, LCC will not reimburse the employee for any purchased content (i.e. videos, music, applications, etc.) that was on the device.

Loss or Theft

Employees responsible for a mobile device must notify IT Services immediately if that device is lost or stolen. IT Services will remotely wipe the device to protect the confidentiality of any data.

Software Updates

Domain Computers (a.k.a. Clients) - These computers are known as "domain" clients because they are joined to the college network and managed over the network. They receive software and anti-virus updates from servers on the college network. Employees responsible for domain laptops, including classroom laptops, must login to the college network with those laptops to receive updates. This should be done as often as possible, but at least once every 30 days.

Standalone Computers - These unmanaged computers are not connected to the college network. They are usually laptops that use the wireless network to access the Internet. Employees with standalone computers are responsible for patching and updating those computers on their own.

Support

IT Services will support LCC-issued mobile devices. Employees should submit a service request and support cases will be created and escalated as needed.

Care for Mobile Devices

The individual is responsible for taking precautions against damage to LCC-owned devices, outside of normal wear and tear. When a device is returned to LCC, it should be in presentable and usable condition with any damages or defects reported to IT Services. Additionally, individuals must take steps toward securing assigned devices at all times (do not leave devices in a car or otherwise unattended).

Personal Use

Users shall follow the Washington State guidelines for the use of state-owned equipment and resources.

Traveling Abroad

Plan Ahead for Trips Abroad

- Using a Smartphone can become expensive when traveling outside the United States.
- Several days in advance of departure, inform the service provider to confirm the device's service plan is set for international use.
- Print hard-copies of your travel itinerary, flight numbers, addresses, and maps. Do not assume you will be able to connect to email or internet for this information.

International Data

- Use Wi-Fi connections wherever possible. Many hotels and restaurants have free Wi-Fi, or charge a fee which is less expensive than the cellular data plan.
- Disable “Cellular Data” and “Roaming”. Enable these settings sparingly and always disable them after use.
- Avoid using the device’s “Wi-Fi Hotspot” capability to connect other devices.
- To track your usage, “Reset usage statistics” on the device upon arrival at your destination. Refer to this screen occasionally to monitor your data and voice usage.
- Turn off or “Kill” apps that you are not actively using.
  - Example: Google Maps continues to consume data after you are done.
- Email
  - Set to “Manual Updates” instead of “Automatic Updates”. Turn off “Push” email.
  - Check email when you are connected to Wi-Fi networks.
  - Wait until you are connected to a Wi-Fi network to download attachments.
  - Do not send attachments or photos unless connected to Wi-Fi.
- Internet / Video / Apps
  - Avoid apps that consume large amounts of data, unless on Wi-Fi.

International Voice

- While on Wi-Fi, use Skype, FaceTime, or similar services which are less expensive compared to regular voice plans.
- Consider using a calling card.
- Keep calls as brief as possible if the options above are not available.

International Texting

- Use email instead of text messages while traveling abroad.

Personally-Owned Devices

Individuals with a personally-owned device which meets IT Services’ standards may choose to connect their personal device to LCC resources such as the public wireless network, web-based email, and cloud applications. Support for personally-owned devices is limited, and the use of such a device to conduct college business comes with guidelines. The individual is expected to protect LCC data.

Security

Individuals who use a personally-owned device must comply with all provisions of LCC IT Security policies. Each individual is accountable and responsible for protecting LCC’s intellectual property, including employee and student information. All users must take reasonable steps to protect personally-owned mobile device against loss or theft and to prevent unauthorized access to, or use, disclosure, or acquisition of, LCC information stored on the device.

The device must meet minimum security requirements. Individuals should use a method such as a swipe pattern, fingerprint ID, or passkey (4 digits minimum) for locking the device.

Should it be deemed necessary for security reasons, IT Services may remotely wipe the device to protect the confidentiality of any data. The individual owner is responsible for maintaining backups of content and data.

LCC reserves the right to prevent access by any personally-owned mobile device running applications that IT Services believes poses a risk to its network infrastructure or may compromise the confidentiality, integrity, or availability of LCC's information. IT Services may limit the use of any device that is "jailbroken or rooted."

Remote Data Wipe

Protecting LCC's intellectual property and the personal information of the college's employees and students is the college's primary concern. As such, IT Services reserves the right to remotely wipe apps and data from any mobile device that is connected to LCC's systems. There are two methods for IT Services to remotely wipe a device.

1. Account Wipe: An Account Wipe will only remove LCC apps and LCC data, including email, calendar items, contacts, applications and documents that are stored on the device. Personal apps and data will remain intact. An Account Wipe feature is not supported by all Mobile Device Management (MDM) solutions.

   If possible, an Account Wipe will always be attempted first. IT Services may initiate an Account Wipe on a personally-owned device in the following circumstances:
   a. Upon an employee's separation of employment from LCC
   b. Upon notification that the device is lost or stolen
   c. When LCC has reason to believe that the information is being, or may be, at risk of misappropriation or other misuse.

2. Device Wipe: A device wipe will reset the device back to its default settings (all data will be deleted). A Device Wipe is immediate and irreversible. Any data or information that has not been previously backed-up or synchronized will be lost. This includes photos, music, applications, emails, text messages, videos, and any other content on the device.

   When an Account Wipe is not possible or is unsuccessful, IT Services may initiate a Device Wipe on a personally-owned device in the following circumstances:
   a. Upon an employee's separation of employment from LCC
   b. Upon notification that the device is lost or stolen
   c. When LCC has reason to believe that the information is being, or may be, at risk of misappropriation or other misuse.

LCC will not be held responsible for the loss of any personal data stored on the device. Further, LCC will not reimburse the individual for any purchased content (i.e. videos, music, applications, etc.) that was on the device.

Loss or Theft

Individuals who access LCC's resources or data on a personally-owned device must notify IT Services immediately if that device is lost or stolen. IT Services will remotely wipe the device to protect the confidentiality of any data.

Public Records

The Revised Code of Washington RCW 42.56.010, known as the Public Records Act (PRA), defines a public record as "any writing containing information relating to the conduct of government . . . ." All communications that further the employer's interests are considered public records. This applies to business and communication conducted using personal cell phones and computers. The Washington State Open Government Resource Manual (chapter 2) states: "Text messages sent and received from a government employee's private cell phone are public records if they satisfy the definition of 'public record' at RCW 42.56.010(3)." Furthermore, the Washington State Supreme Court determined that:

> . . . **employees are responsible for searching their files, devices, and accounts for records responsive to a relevant PRA request. Employees must produce any public records (e-mails, text messages, and any other type of data) to the employer agency** (emphasis added). The agency then proceeds just as it would when responding to a request for public records in the agency's possession by reviewing each record, determining if some or all of the record is exempted from production, and disclosing the record to the requester . . .
>
> Where an employee withholds personal records from the employer, he or she must submit an affidavit with facts sufficient to show the information is not a "public record" under the PRA. So long as the affidavits give the requester and the trial court a sufficient factual basis to determine that withheld material is indeed nonresponsive, the agency has performed an adequate search under the PRA. When done in good faith, this procedure allows an agency to fulfill its responsibility to search for and disclose public records without unnecessarily treading on the constitutional rights of its employees. (*Nissen v. Pierce County*)

Support

IT Services does not provide support for personally-owned equipment.

Application of LCC Policies

All LCC policies apply to individuals who use a personally-owned device to access LCC's information or information systems, or to conduct LCC business.

Acronyms and Definitions

- Account Wipe: An Account Wipe will only remove LCC apps and LCC data, including email, calendar items, contacts, applications and documents that are stored on the device. Personal apps and data will remain intact.
- Device Wipe: A Device Wipe will reset a mobile device back to its default settings. All data will be deleted.

- Domain Client or Computer: A computer that is a member of a network domain. It is managed with network policies and receives automatic software updates over the network.
- Family Educational Rights and Privacy Act (FERPA): FERPA is a federal privacy law that gives students certain protections with regard to their education records, such as grades, transcripts, disciplinary records, contact and family information, and class schedules.
- Jailbroken: A mobile device that has been modified to remove restrictions imposed by the manufacturer or operator, usually to allow the installation of unapproved or unauthorized software.
- LCC Data: Any information used in the process of conducting business for LCC. This includes email messages and attachments, calendar appointments, contact information, instant messages, and any other pertinent electronic information for executing one's specific job duties within the college.
- Mobile Device: Any portable technology capable of accessing or transmitting data wirelessly.
- Mobile Device Management (MDM): An application used to monitor, manage and secure multiple mobile devices and operating systems deployed in the organization.
- Personal Data: Any information specific to an individual, but not relevant to specific job duties within the college.
- Public Record: Any writing containing information relating to the conduct of government (RCW 42.56.010). Any record that an employee prepares, owns, uses, receives or retains within the scope of employment, including but not limited to texts, voice mail, email, instant messaging, calendars, photos, and video. All data stored on LCC-owned mobile devices is discoverable, and, therefore, is not private by nature.
- Rooted: See JAILBROKEN
- Standalone Computer: An unmanaged computer that is not connected to the college network. A standalone computer does not receive software updates over the network. Therefore, users of standalone computers are responsible for managing software updates on their own.

1600 Maple Street, Longview, WA 98632
lowercolumbia.edu