Safe Use and Handling
Staff Devices

Avoiding BitLocker Issues

BitLocker is a full disk encryption feature included with select versions of Windows. In addition to your username and password, this feature will help prevent unwanted access to the data stored on your laptop's hard disk.

While BitLocker was designed to operate unnoticed by the computer user, there is one way in which this feature can be triggered by accident. Once in effect, it will prevent further use of the computer until it is unlocked by the Technology Department.

Improper Shutdown

Your computer should always be shut down by clicking on the Windows key and selecting "Power Off" or "Shut Down." Never press and hold the power button. While this will shut down the computer, it may also invoke BitLocker. Once the BitLocker lock is initiated, you will be unable to log on or use the computer without Technology Department Assistance.

Windows Updates

When your laptop is off of the ORTN network, it can still receive updates. A best practice is to ensure your computer's power adapter is plugged in at night. This will ensure the battery is fully charged when you return to school in the morning.

In addition, if your computer has received Windows updates, it may require a reboot to finish installing them. If this is the case, the option to "Install Updates and Shutdown or Restart" will be visible when the Windows key is pressed. Once a reboot is initiated, please be patient and allow the process to finish. Many Windows updates are installed on shutdown but must be configured on the reboot. DO NOT shut down the computer manual as this may result in loss of data or use of the computer.

Improper Transport or Handling of Devices

Whenever possible, it's best practice to carry your device using a carrying case or a backpack with a designated laptop sleeve.