

## Administrative Procedure 144

---

### 144 - REMOTE LAPTOP USE

#### Background

Wild Rose School Division believes that the use of laptops both inside and outside of the Wild Rose Network is an essential business and educational function for our staff. Wild Rose School Division has provided the means in which individuals have the ability to use laptops both on and off of the Wild Rose Network. Wild Rose School Division has installed district wide anti-virus, and content management measures to protect the hardware, software, and data assets of Wild Rose Public that reside on the Wild Rose Network.

The use of laptop computers that may be directly connected to networks or an internet connection other than the Wild Rose Network, presents a significant risk to Wild Rose School Division's data assets and the Wild Rose Network. Mitigating this risk requires both good tools and prudent action on the part of laptop users. This Laptop procedure outlines the measures laptop users must take to mitigate the risk of damaging the Wild Rose Network through the introduction of a virus, Trojan, spyware, or other malicious infection and outlines measures to protect Wild Rose Public Schools owned confidential information.

#### Procedure

##### 1. Non-Permitted Use

Due to the significant risk of virus or malware infection, a direct or indirect connection to the Wild Rose Network by any computer not owned by Wild Rose Public Schools is not permitted.

Home wireless: Home-based wireless network connections are inherently insecure and should be avoided. However, provided the level two users adhere to the level two procedures on confidential files, a wireless network intrusion should not cause serious harm.

##### 2. Remote Use Procedures

With respect to Wild Rose School Division owned laptops, two levels of remote use have been defined. The term "remote use of a laptop" refers to any use of a laptop that is not directly connected to the Wild Rose Network. Each level requires specific actions on the part of the laptop user to ensure ability to login, protection of confidential data, and the protection of the Wild Rose Network.

###### a. Level One

Level One involves remote use of a Wild Rose Public Schools laptop which is never connected to any other network. Prior to the laptop being taken out of the school for remote use the users of the remote laptop must follow the outlined procedure.

- i. Login to the laptop while the laptop is connected to the Wild Rose Network, this will ensure that the user will be able to login to the laptop when that laptop is removed from the network.
- ii. The user must be the last person to have logged into the laptop while connected to the Wild Rose Network.
- iii. Any documents to be worked on must be accessed through a plug and play memory key.

###### b. Level Two

Level Two involves remote use of a Wild Rose Public Schools laptop which has been connected to any other network other than the Wild Rose Network (hotel, home, other school division, Alberta Education, etc.).

Level Two represents the most significant risk of remote laptop use. Therefore it is imperative that Level Two users adhere to the following procedure:

- i. Level Two users need to ensure that while connected to a remote network for internet connectivity, the USB memory key is not plugged into the laptop and the user is not working on confidential files. The USB memory key should only be plugged into the laptop and confidential files should only be worked on when the remote network has been disconnected.
- ii. Since Level Two use involves exposing the laptop to a raw unprotected Internet connection (connections not afforded the protection measures provided on the Wild Rose Network), Level Two users must disinfect any laptop used prior to reconnecting that laptop to the Wild Rose Network.

To disinfect, Level Two users need to do the following:

1. Ensure that you are connected to the internet and have a live internet connection
2. Complete a live update of the Symantec anti virus software:
  - a. Double click on the Symantec antivirus shield displayed in the right hand section of the task bar or choose Start, Programs, Symantec Client Security.
  - b. Click on the Live Update button in the Symantec window.
  - c. On the live update window click on next, next and then finish.
  - d. Wait for the update to say it is complete.
  - e. Once you see the message "Update Now has been successfully completed." Click the Ok button.
3. Disconnect from the remote network.
4. Sometime before you re-connect to the Wild Rose Network, you need to do a full scan of the laptop. If you use a jump drive or memory key, you should have it connected for the scan.
  - a. Double click on the Symantec antivirus shield displayed in the right hand section of the task bar or choose Start, Programs, Symantec Client Security.
  - b. Click on the scan folder in the left window of the Symantec window.
  - c. Choose full scan.
  - d. Click the scan button.
  - e. Allow the scan to complete. This could take quite a while so you may want to leave the computer unattended.
5. Once the scan is complete, check the results: If a virus has been found and it was not removed successfully, return the laptop to Technology Services immediately; if no viruses

were found, or if those found were all successfully removed, you are clear to reconnect to the Wild Rose Network.

### **Appropriate Use Policy**

Users are reminded that use of laptops offsite and all Wild Rose Public Schools Technology Resources are required to be in congruence with the terms of The WILD ROSE PUBLIC SCHOOLS Acceptable use Policy.

### **Windows File Synchronization**

Windows file synchronization of home directories will not be permitted due to the fact that the offline data on the laptop can not be properly secured incase of loss or theft of the laptop.

### **Security of Information Resources**

Transportation of documents on USB memory keys must also meet the Security of Information Resources administrative procedure.