Sierra in the Wild Procedures

The following procedures allow staff at OWLSnet member libraries to use Sierra outside of a library. These procedures are in place to protect patron privacy and member library data in the event that a laptop is lost or stolen. To protect the data, the laptop must be shut down while in transit and whenever it is unattended. If a laptop is lost or stolen while logged on, the data will be vulnerable.

Sierra in the Wild Requirements

Sierra in the Wild requires the use of a dedicated laptop that is:

- Library owned (multiple libraries may share a single laptop used for this purpose)
- For library staff use only (not used by the public or family members)
- Running Windows 10 Pro with BitLocker encryption

All library staff using the laptop must agree to the following:

- The Sierra in the Wild laptop will only be used by staff. It will not be used by members of the public or family members.
- The laptop will be shut down whenever not in use by library staff, including during transport to and from the off-site location or when unattended by library staff, no matter how briefly.
- Staff will not check the "remember me" option in Sierra.
- Staff will memorize the BitLocker encryption password and will not have a written copy outside of a secure location in the library.
- Staff will immediately report a missing laptop to the library Director and the OWLS Network Manager.

How to use Sierra in the Wild

First time users

- Verify that you can meet the above requirements. OWLSnet staff will work with libraries to install Sierra and VPN software, then encrypt the laptop with BitLocker.
- Sign the Sierra in the Wild Agreement and send it to OWLS. Keep a copy of the agreement in the laptop case.

Scheduling a remote site visit

- Send an email to OWLSnet Help telling us when you plan to use Sierra in the Wild. OWLSnet staff will verify that we have VPN licenses available for that date and time.
- If you will be using a network that isn't open to the public, such as a school network, obtain authorization from the network administrator. They may need information about your laptop to grant authorization.
- Memorize necessary passwords.

At the remote site

- Unencrypt the laptop with BitLocker password.
- Log in to the VPN (see OWLSnet Manual for documentation).
- Log in to Sierra.

Before leaving the remote site and whenever laptop is unattended

- Log out of Sierra.
- Log out of the VPN.
- Shut down the laptop to re-enable encryption.

Sierra in the Wild Agreement

I agree to the following:

- The Sierra in the Wild laptop will only be used by library staff. It will not be used by members of the public or family members.
- I will make sure the laptop is shut down whenever it's outside of the library and not in use by library staff, including during transport to and from the off-site location and when unattended.
- I will not check the "remember me" option in Sierra.
- I will memorize the encryption password and will not have a written copy outside of a secure location in the library.
- I will immediately report a missing Sierra in the Wild laptop to my library Director and to the OWLS Network Manager.

_____ _____

(signature) (date)

Please keep a copy of this agreement in the laptop case.