Stone County School District

Security Policy for District Owned Portable Computing Devices

Introduction

Mobile computing devices offer staff the ability to be more productive while on the move. They offer greater flexibility in when and where staff can work and access information, including information on the school districts network. However, network-enabled portable devices also pose a serious risk of data theft, unauthorized access to the district's network, as well as increased risk of viral and spyware infection district wide.

Any device that can access the school systems network must be considered part of that network and therefore subject to policies intended to protect the network from harm. **Any** portable device considered for connection to the SCSD network must be approved and certified by the Technology Department.

Protecting the Portable Device (and the SCSD network)

As a minimum, in order to qualify for access to the district's network, the device must meet the following criteria:

1. Device configuration must be reviewed and approved by Technology Services personnel.

2. The devices firewall (if applicable) shall remain active, while on or off school district property.

3.) Antivirus software (if applicable) must be installed and up to date. Only district approved anti-virus, anti-spyware and anti-malware applications may be installed and used.

User's Responsibilities (This policy was written with the understanding that a single user may have not just one but many district owned portable wireless devices assigned to them.)

1. The assigned user of the device(s) is responsible for network (online) security of the device(s) whether on school property, at home, or on the road.

2. Use of insecure public internet services is prohibited, as they do not offer adequate protection for the user. This does not include internet services provided directly to your home or via hotel access if on school related travel.

3. Tech Services personnel are not responsible for establishing or supporting your device(s) off-campus internet connection.

4. The assigned user may not install any additional software on the device(s) without prior approval from the Technology Department. A valid software license will be required prior to installation of software applications.

5. Self-recorded CD's and/or DVD's may not be used in district owned portable computing device(s) nor should they be brought on campus for use in school computer systems without being first checked by the Technology Department. Doing so may result in the termination of the user's right to take their device(s) off school property.

6. **Important!** Protection of the device(s) from damage, loss, theft or other physical abuse is the **assigned user's responsibility**.

7. No individual, other than the assigned user, is authorized to use a school-owned device(s) while located off school property.

Security Audits

The Technology Department reserves the right to audit any portable computing device, personal or otherwise, used for school business to ensure that it conforms to the requirements mentioned in the district's Acceptable Use Policy. They may also deny network access to any device which has not been properly configured and certified by the Technology Department.

Declaration of Understanding

I have read, understand, and agree to adhere to Stone County School Districts Security Policy for Portable Computing Devices. I also understand that I may be held financially responsible for any damage to, or loss of, an assigned device(s) should it occur while OFF school property. I also understand that I may be held financially responsible should loss or damage occur while ON school property if said property was left in an unprotected environment.

Name (Printed): _____

Name (Signed): _____

Date: _____