ADMINISTRATIVE PROCEDURE NO.160

COMPUTER SYSTEMS NETWORK

Background

The Division provides networked computer systems, including access to the Internet, to promote educational excellence, to increase alternate sources of information, to promote resource sharing, to further innovation in instruction and communication, and to prepare students for their future. The Division network systems include all hardware, software, data, communication lines and devices, printers, servers, desktop computers, E-mail, Internet access, and local school networks. To maintain a secure Division network, systems and services that require Internet access where a login password is required, the access to these wireless networks has been restricted to assist in network security and appropriate content filtering. To prevent unauthorized access to the Division Network and to provide a reliable and optimally operational network, a level of network security is required.

Procedures

1. All users of the Division's computer systems and network resources have the responsibility to ensure its overall security and to behave in a manner consistent with this administrative procedure.

2. No staff, student or community users shall connect any device into the Division wired network without authorization.

3. Staff, students or community members are prohibited from installing or using software or hardware that bypasses any network security measure or bridges a foreign network to the Division network (i.e. VPN tunnels).

4. Wireless network connections are permitted according to Division protocol. When logging in, a secure password must be used.

   4.1 Users should keep the login name and password secure. Passwords are not to be shared unless authorized.

   4.2 Password requirements.
   - 4.2.1 No dictionary words, proper nouns, or Foreign words,
   - 4.2.2 Change the password when you are first given your account,
   - 4.2.3 No personal information in your password,
   - 4.2.4 Don't reuse passwords
   - 4.2.5 Change passwords regularly. Currently the system requires user to change it every year,
   - 4.2.6 Use pass phrases to create a more complex password, example "The sky is blue!)

4.2.7 Passwords must contain at least 8 characters from three of the following five categories:
- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharps, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

5. The Division will continue to support a *PC based computer platform*. Other devices may be supported if time allocation and training is available.

5.1 IT department will maintain a list of devices (Appendix A) and level of support to be provided for each device.

5.2 A request for new devices to be added to the list can be made by completing the form in Appendix B and submitting to the Superintendent or designate.

6. Several wireless networks have been created and are accessible in Division facilities. Different user groups will require a specific wireless login and password. Staff and students will be required to use an active directory username and password. Content filtering will be based on user group login.

7. To ensure computers are operating on a stable network with appropriate software, the IT Department will order all division owned computers on a yearly basis. This will minimize the number of makes and models that require support from the department and ensure a stable image that will function on all computers.

7.1 The IT Department budget will allocate funding to replace division owned desktop and laptop computers.
- 7.1.1 Computers will be replaced on a 5 year cycle.
- 7.1.2 Replacement will be based on a student computer ratio of 4:1 for elementary and middle schools and a 3:1 ratio for high schools.
- 7.1.3 Student enrolment projections will be based on the Division's Three Year Capital Plan.
- 7.1.4 Schools can request either laptop or desktop computers when their replacement time occurs in the cycle.

7.2 Non-school based departments will need to ensure budget allows for computer replacement following the same cycle.

7.3 Division IT staff will support the configuration/ imaging of these devices as follows:
- 7.3.1 Desktops- imaging and hardware support. Repairs to computers due to student vandalism will charged back to the school.
- 7.3.2 Laptops- imaging and hardware support. Repairs to computers due to student vandalism will charged back to the school.

7.4 Schools may keep or request decommissioned computers that are over 5 years old.
- 7.4.1 Computers will be allocated on an as is condition.
- 7.4.2 Schools will be responsible to ensure appropriate computer furniture is in place to receive these computers.
- 7.4.3 Any costs associated with additional data drops or power outlets are the school responsibility.
- 7.4.4 Imaging and/or hardware support may not be available for these devices. When they are deemed unusable, they will be recycled.

8. To provide equitable access of technology for students, and / or focusing learning projects including staff, schools may invest with their school allocated funds into technology. These devices may include, but are not limited to iPods, iPads, netbooks, Chromebooks, and laptops. Devices need to be purchased through partnership with the IT department.

8.1 Schools will request their non-PC based devices to be connected to the RDCRD wireless network using the IT Help desk supplying the following information.
- Wi-Fi MAC addresses.
- Filtered as a staff or student device.
- Device owner.
- Type of device.
- Phone number (for phone access).

8.2 The ongoing maintenance, repair and replacement costs for these devices are supported by the purchasing school.

8.3 Division IT staff will support the configuration/ imaging of these devices based on time allocation and individual training. Not all devices can be fully supported. A list of supported devices is in Appendix A.

9. To provide seamless integration of technology from school to home, staff owned devices are allowed to connect to the Division wireless network. In order for the proper content filtering to be applied, each personal owned staff device requires registration.

   9.1 Staff will request their personal device to be connected to the RDCRDSTAFF wireless network using the IT Help desk supplying the following information.
   - Wi-Fi MAC addresses.
   - Filtered as a staff or student device.
   - Device owner.
   - Type of device.
   - Phone number (for phone access).

   9.2 Staff will be able to log onto the RDCRDSTAFF wireless using their Active Directory (Computer Login) username and password. Content filter will be applied based on this administrative procedure.
   9.2.1 Staff owned devices can connect to the internet through a division firewall but does not connect directly to the internal network.

10. To provide seamless integration of technology and enhance student collaboration from school to home, student owned devices are allowed to connect to our wireless network.

    10.1 In order for school to begin the Bring Your Own Device (BYOD) program in their school the following criteria must be met.
    10.1.1 All students must complete a digital citizen course.
    10.1.2 Equitable access for all students is to be addressed at the school.
    10.1.3 Staff PD to ensure effective teaching strategies using BYOD.
    10.1.4 Checklist completed, signed off and submitted to the Superintendent or designate.

    10.2 Students will be able to log on the WSTUDENT wireless using their active directory (Computer login) username and password. Content filter will be applied.

11. There are portions of the network identified as critical or core to the operation of the Division. Uninterruptable Power Supplies (UPS) are provided to servers, network switches, and phone system to prevent damage to short duration power spikes as well as longer duration power outages

    11.1 Battery powered backup should provide power to servers, network switches, and phone system for up to 15 minutes.

11.2 The UPS system protects critical equipment from source power disturbances and outages, load faults. Under no circumstances should anyone connect a device that draws power from the UPS without consent from The IT department.

12. Web portal access is provided to staff to facilitate access to the Division's internal network. Access can be from home or from other networks while traveling. The portal provides a secure connection through a virtual window to the user. This virtual window isolates the Division's network from the outside network being used and protects the Division network from potentially harmful software.

    12.1 Since the devices connecting to the Web Portal includes a varied selection of possible devices, limited support can be provided in assisting staff connections.

    12.2 Help desk support is provided during IT staffing hours of 8 AM to 4:30 PM.

    12.3 The responsibility is on the staff member to troubleshoot connection issues with information provided by the IT Department.

    12.4 A connection to the Web Portal my not be possible from all devices,

    12.5 This service is provided as is and there is no guaranty that every configuration used at home will be able to connect.

13. The purpose of E-mail is to facilitate communications in support of research and education by providing the opportunity for collaborative work. E-mail will allow staff and students to interact with a variety of networks and computers for educational purposes.

    13.1 All staff shall complete the Acceptable Use Agreement (Form 32). This agreement will be returned and kept on their permanent personnel file.

    13.2 Principals shall ensure that volunteers who have access to the Internet/E-mail system complete an Acceptable Use Agreement form each year. This shall be kept on file at the school.

    13.3 Personal storage devices may only be used on the network computers with the prior approval of the teacher in charge.

        13.3.1 Staff in charge of student users will ensure, as much as is practicable, that students are closely supervised while they are on the Internet; and

13.3.2 continually educated in the responsible use of the Internet.

13.4 Violation of the Division's Acceptable Use Policy may result in:

13.4.1 restricted network access;
13.4.2 loss of network access;
13.4.3 disciplinary action;
13.4.4 legal action.

14. While accessing the internet, certain websites may contain material that is morally offensive or contradicting the beliefs of the Catholic Church and Catholic Education. All networks maintained by Red Deer Catholic Regional Schools accessible by students and staff will have various levels of content filtering applied.

14.1 Users are grouped into 4 basic categories for the purpose of content filtering. Elementary students, middle school students, high school students, and division staff.

14.2 All Http and Https connections are logged.

14.3 Websites containing pornographic, sex and online gambling content shall be blocked for all user groups.

14.4 The school principal shall determine which websites shall be blocked or unblocked for users using the following process.
14.1.1 Teachers request to their principal for a website to be unblocked for educational purpose.
14.1.2 Principal shall review site to ensure age appropriate and educational content.
14.1.3 Principal shall request the IT Department to unblock a website using the IT Help desk.
14.1.4 Principal shall inform other principals of the same user group of the unblocked site. A detailed document list containing a list of blocked and unblocked categories can be found in DivisionShared\IT Department\Websense Categories. A detailed document list containing a list of unblocked sites can be found in DivisionShared\IT Department\Unblocked Website.
14.1.5 Principal and teacher shall monitor site to ensure age appropriate content and request blocking if needed.

14.1.6 In some instances, certain websites may cause higher than normal security risks to the division network. In these cases the IT Manager, Superintendent or designate and the Principal will review the request.

15. The division phone system consisting of CISCO phones, switches, and servers are supported by the IT Department.

15.1 All effort will be made by the IT Department to keep the phones running as long as possible during a power failure,

15.2 Current battery backup time during a power failure is 15 minutes.

15.3 Cost of phone replacement and any work required outside of the IT Department will be school costs.

15.4 The Paging and Security Systems are maintained by Maintenance. IT will assist in troubleshooting issues with the Paging and Security systems accessed through the phone system.

ADMINISTRATIVE PROCEDURE NO. 160

Appendix A

List of currently supported devices:

Desktops and laptops from yearly divisional purchases running Windows 7 Enterprise are supported by the IT Department. These devices are purchased yearly in large quantities to minimize the number of models, thereby reducing support costs.

Devices with minimal support that IT staff may support:

1) Apple configurator to manage iPads and iPods
2) iOS devices such as iPads, iPods, iPhones and Chromebooks (limited to connecting to our wireless and possible simple issues). No support for individual apps on the devices.
3) Mac computers, desktop or laptops. No hardware support on all Apple products.
4) other windows devices and netbooks.

No current support available from IT for the following devices. Devices will be connected to the appropriate wireless if provided with the machine's Wi-Fi MAC address:

3) Android devices
4) No hardware support on all Apple products. Recommended to contact Apple directly for support
5) all other devices

ADMINISTRATIVE PROCEDURE NO. 160

Appendix B

Request for Additional Devices to be Supported

Please complete the following form and submit to your Principal for approval. Requests will be reviewed on a yearly basis to determine whether the requested device will be added to the list.

Name:_____ Date:_____
School: _____

Device requested for Division IT Support:_____
_____
_____

Educational reason why this device needs Divisional support: _____
_____
_____
_____
_____

_____

For administrative use only
Principal Approval Yes No Signature: _____
Date request submitted to Superintendent or designate:_____

APPENDIX ‘A’

Phone Plans- United States and International Travel

When traveling outside of the country, it is important to know what usage will be required from the phone. Phone usage without a pre-purchased plan is considerably more expensive.
There are 3 areas of phone usage and plan costs to be aware of:

1. Phone Plan- a selected US or international travel plan which would give a define number of minutes on the phone. Any usage above the plan allotted time will be charged by a minute rate (usually at a lower cost than without any plan). Without a plan, there will be higher costs for long distance as well as roaming charges.

2. Text Plan- a US or international text plan is available for a defined number of text messages. Any text messages above the selected plan are charged extra. Text messages without a plan are charged per text as well as including roaming charges.

3. Data Plan- a US or international travel plan can be purchased for for different amounts of data usage. Usage above this amount is charged per megabyte.

In all cases, the user must know the amount of use/time that will be used by the electronic communication device. In most cases, it is recommended to turn Data Roaming off and use only when there is access to Wi-Fi. To turn off data roaming go to:
Settings> General> Network> Data Roaming – turn to OFF.

Using a Division cell phone outside of Canada can be expensive. Additional phone plans and any costs incurred over and above the plan for personal travel will be at the cost of the user.

A phone can be reset to keep track of data and voice minutes under:
Settings> General> Usage – press Reset Statistics.