Red Deer Catholic Regional Schools

Ecole Camille J. Lerouge will be entering into a new and exciting technology development for our students. We will be allowing students to bring in their own technology from home and connect to the internet through our wireless network. While we understand that there are considerable advantages to this development, we also see a number of concerns that we will address in order to ensure a safe environment for your children. As a school we are committed to the safety of our students while they are in our care. In order to do this we have set up a number of precautionary measures that will enable us to continue providing a worry free technology environment for your children.

Rapid advances in digital technologies are dramatically changing how society communicates, interacts, and shares information. We believe that the access to wireless Internet by student devices will increase a student's ability to access research information, creatively express their knowledge, collaborate and communicate with peers and to extend their learning outside the classroom.

Once connected, digital devices will have the same Internet restrictions that we impose on students in the computer laps and mobile laptops. Content filters, restriction to online applications and blocked websites will continue to be part of our school's safety process. In the classroom, teachers will limit the use of technology and impose rules with regards to student access and use. Finally, wireless access will also be restricted to the school hours of operation.

The parent permission form attached to this document is essential for your child's use of their own technology. Without it they will not be allowed to use their own digital devices. From laptops to smart phones, students will have the ability to bring in a device that allows them to connect to the Internet wirelessly and safely. It is important for parents to know that **the school is not responsible for any lost, damaged or stolen digital devices while they are at school**. Each device will be used at the user's own risk.

Ensuring equality of student access to technology is something that we are conscious of. We understand that some students will not have access to home digital devices and therefore the school will provide access for them. As a school we do not want to create an inequality within our students in terms of who can and who cannot afford this type of technology. We wish to state again the primary goal of technology is to enhance student learning through safe use of current, practical and relevant technology that meets our mission as a Catholic school division and the educational needs as defined by Alberta education.

Some examples of Personal Devices include laptop computers, netbook computers, tablets (iPad, Kindle), eReaders (Nook, Kindle, iPad), MP3 players (iPod), smart phones (iPhone, Android) . Please read through the following pages, and then detach, sign and return the agreement on the last page.

Rationale

Research indicates that students who have access to technology on a regular basis show a significant improvement in their learning skills over students who do not have regular access. With this in mind, every effort will be made to provide access to quality resources that will hopefully reshape how students learn. Many students that we serve own devices such as smart phones, tablets, laptops, and e-readers that can supplement their learning if used appropriately in the classroom. The purpose of the Bring Your Own Device (BYOD) initiative is to move further into the digital learning age by facilitating safe and productive use of such devices and thereby to empower students to take more active ownership of their own learning.

Types of Devices

Many different types of devices qualify for inclusion as Personal Devices. Smart phones, tablet computers, e-readers, and laptop computers are just some examples. Even certain handheld gaming devices have web-browsing components that may make them suitable for educational use in a BYOD initiative. The only requirement for a device that needs network access is that it be able to connect to a secured Wi-Fi network. The only requirement for a device that does not need network access is that it must have the potential for legitimate educational uses. Students and their parents must make reasoned and informed decisions about which devices may or may not be appropriate to bring to schools given the rest of these guidelines.

Acceptable Use

Providing opportunities for students to use their devices for educational purposes shall fall under the professional discretion of the classroom educator. The educator may allow or disallow students in classrooms to supplement RDCRS device usage or curricular material usage with devices which students bring to school.

Sample uses would be to allow students to perform research via websites, to participate in informal assessments via electronic polling or surveys, to read electronic texts, and to send messages to educators via educationally-appropriate social networks – all falling under educational use as directed by the educator.

No element of the BYOD initiative shall require any classroom educator to provide opportunities for students to use their own devices; the classroom educator shall exercise professional authority to allow or disallow such use in all cases. Furthermore, no classroom educator shall create an assignment, assessment, or learning experience in which student devices are required; RDCRS devices will be available to students in such cases when technology use is required in a learning environment and no suitable student devices are available.

No students shall be required to share their devices with others students. To avoid loss, theft, and damage, sharing of student devices with other students is not recommended.

Sound should be muted at all times in the classroom unless permission is obtained from the teacher for instructional purposes. Personal headphones or ear buds must be used for activities that have sound associated with them, which shall be provided by the student.

Inappropriate media may not be displayed on screen savers, desktop wallpaper or backgrounds while in use at school. Presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drug, and gang related symbols, pictures or applications may result in disciplinary action.

Parent / Guardian and Student Agreement

In order to participate in the BYOD initiative, students and their parents or guardians must review and agree to the guidelines and acknowledge consent by signing and returning the BYOD Agreement Form to their schools. No student shall be permitted to participate without the signed agreement.

Responsibilities – Students

Students shall adhere to the agreements made in the Personal Device Usage Agreement and the Student Acceptable Use of Internet/Email Agreement. Students shall use their devices responsibly and for educational purposes under the direction of the classroom educator. Students shall take all reasonable steps to keep their devices physically secure and free of malware, e.g. running up to date anti-virus software and using a lock code or device password if possible. Students shall ensure that their BYOD privileges are not revoked by exercising good judgment with respect to their use.

Responsibilities – Parents / Guardians

Parents/guardians shall adhere to the agreements made in the Personal Device Usage Agreement and the Student Acceptable Use of Internet/Email Agreement. Parents/guardians shall help their children to take all reasonable steps to keep their devices physically secure and free of malware, e.g. running up to date anti-virus software and using a lock code or device password if possible. Parents / guardians shall encourage their children to exercise good judgment with respect to device use and shall not unduly attempt to contact students during instructional time via text messages, E-Mails, or phone calls that would disturb the classroom learning environment.

Responsibilities – Educators

Educators shall use sound professional judgment when creating opportunities for students to use their devices for educational purposes. Such opportunities shall always allow for safe and productive learning environments to be maintained. Educators shall disallow student device usage in instances when safety and productivity would be compromised. Educators shall make clear their stances on student device usage in their classrooms. Educators shall communicate appropriately with administrators and parents if students violate the letter or spirit of the BYOD initiative.

Responsibilities – Administrators

Administrators shall continue to support safe and productive learning environments by encouraging sound professional judgments by their educators with respect to opportunities for student device usage. Administrators shall encourage innovative uses through instructional conversations with educators. Administrators shall respond effectively to student disciplinary issues with respect to inappropriate device usage.

Potential Consequences of Misuse

Above all, Ecole Camille J. Lerouge strives to maintain safe and productive learning environments. Students are therefore expected to adhere to the policies, procedures, and guidelines established for safety and productivity at all school sites. Students that choose to ignore, circumvent, or directly counteract those efforts with respect to their device usage will face consequences for doing so. These consequences may include but are not limited to revocation of BYOD privileges, confiscation of devices (to be returned only to parents or guardians), or suspensions. Administrators shall determine appropriate consequences for students who misuse devices. Classroom educators have immediate authority to revoke BYOD privileges in their own classrooms and may recommend to administrators full revocation.

Loss, Theft, and Damage

Students are solely responsible for the care of devices they choose to bring to school. RDCRS shall not be held responsible for lost, stolen, or damaged student devices nor for malware devices may inadvertently acquire via the RDCRS wireless network. Students are strongly encouraged to keep devices secured at all times when not in use. Under no circumstances should personal devices be left in unsupervised areas. Any personal device left in an unsupervised area is in danger of being stolen. No students shall be required to share their devices with other students. To avoid loss, theft, and damage, sharing of student devices with other students is not recommended. Lock codes or device passwords are encouraged.

Technical Support

Students shall be responsible for their own technical support and for making sure that they have the most up to date software installed for their own devices' protection. RDCRS staff members shall not provide technical support for any non-RDCRS-owned technologies. This prohibition includes troubleshooting student devices for software and hardware issues and removing malware from devices. However, electronic and printed tip-sheets for connecting student devices to the RDCRS wireless network may be made available.

Technical – How to Connect to the RDCRS WSTUDENT Wireless Network

The following are steps to take for connecting common operating systems / devices to the WSTUDENT network.

iOS Under Settings, select Wi-Fi. Select WSTUDENT. The device will then attempt to connect. Students use their normal computer account name and password.

Android Under Settings, select Wireless controls or Wireless & Networks and then Wi-Fi Settings. Select WSTUDENT. The device will then attempt to connect. Students use their normal computer account name and password.

Mac OS X Click the Wi-Fi icon in the upper right and select WSTUDENT. The device will then attempt to connect. Students use their normal computer account name and password.

Windows Click the Wi-Fi icon in the system tray and select WSTUDENT. The device will then attempt to connect. Students use their normal computer account name and password.

Technical – Networks

Devices That Need Network Access and Devices That Do Not

The BYOD initiative applies to both devices that need wireless network access and devices that do not. For example, a Kindle e-reader that already has books loaded would not need wireless network access, but the guidelines with respect to appropriate use, charging, loss, etc. still apply. Devices that need wireless network access will have a network available as outlined below.

RDCRS vs. non-RDCRS Networks

Student devices shall be permitted to connect to the WSTUDENT network that is provided by RDCRS when students are directed to use their devices for educational purposes under the supervision of the classroom educator.

Student devices may already have access to non-RDCRS networks such as 3G/4G/LTE mobile phone networks. Such networks should not be accessed by students when their devices are being used for educational purposes under the supervision of the classroom educator – all educational use should flow through the WSTUDENT network. RDCRS shall not be held responsible for content viewed or charges accrued on student devices via such non-RDCRS networks and students may face disciplinary actions for accessing such networks inappropriately.

Filtering

The wireless network provided by RDCRS for student devices filters content consistent with the network filtering provided to RDCRS-owned devices. Additionally, material considered to be harmful to network security such as websites that spread viruses or other malware are blocked. However, no filtering system is perfect and therefore if students find sites containing inappropriate content they should inform their classroom educators.

Technical – Connecting, Charging, and Software

Charging

Students should ensure that their devices are charged prior to bringing them to school. Students shall not attempt to charge their devices in RDCRS buildings. Attempts to do so would raise issues related to electrical circuit overloads, fire safety, and safety of physical movement in common spaces.

Software Installation

While educators may recommend certain software for student use, including apps for mobile devices, no educator shall *require* the use of specific software on student devices. Additionally, no Ecole Camille J. Lerouge staff member will install or provide licensing codes for software for student devices. Ecole Camille J. Lerouge and its staff members shall not be responsible for any negative consequences to student devices caused by running specific software.

Frequently Asked Questions for Parents / Guardians

Do I have to supply a device for my child to bring to school?

No, participation in the BYOD initiative is completely voluntary. Ecole Camille Lerouge will continue to supply devices to students when technology is to be infused in a particular learning experience.

Should I go out and buy a laptop or tablet for my child?

Before making any purchase specifically for BYOD participation, you should have a conversation with your child's educators to determine how frequently devices may be used and for what purposes. Ecole Camille Lerouge cannot recommend one device over another, but all students will have Ecole Camille Lerouge devices available when technology is to be a part of instruction. No student will need a personally-owned device to get the full benefit of Ecole Camille Lerouge educational experiences.

Do I need to buy certain software for my child's device?

No specific software will be required by classroom educators. Educators will attempt to have students leverage whatever software they may have available on the device; if needed software is not available, a Ecole Camille Lerouge device with the software can be substituted.

When can my child use his or her device at school?

Each classroom educator has the discretion to allow or disallow any device during any part of the class session. You can speak with your child's educators for general rules. Use of devices outside of class sessions (such as during class changes or at lunch) are at the discretion of the school administrators.

What happens if my child runs up cellular network charges while using a device in school?

RDCRS supplies a Wi-Fi network that is free for students to use as a benefit of their participation in the BYOD initiative. Students should not use their own cellular networks / data plans while in school, and RDCRS is not liable for any charges that accrue if they do so.

What about Internet filtering? Can my child accidentally access websites that are not appropriate for school?

Content filters, restriction to online applications and blocked websites will continue to be part of our school's safety process. However, no filtering system is perfect and therefore students may inadvertently visit sites with inappropriate content. If that happens, students should inform their classroom educators.

Is it possible for my child to perform all their work and turn in all their assignments using his or her device?

No, it is not. Much of the work students will be assigned must be done by hand or using tools not available on many mobile devices. In some cases, the classroom educator may have a system for handing out and accepting work electronically, but that will vary by school, by educator, and by assignment.

What about my child texting and sending E-mail?

Communications by students such as texting and E-mail may in fact be allowed or disallowed depending on the nature of the work going on in a classroom. The educator will make clear to all students when such use is appropriate and when it is not.

May I text, E-Mail, or call my child during school hours?

Communications to students such as text messaging, E-mail, and phone calls frequently disturb the learning environment of the classroom. Please refrain from contacting your child in those manners during instructional time. Emergency contacts can always be made through the school office.

Can my child take his or her e-reader to school to read during the day?

E-readers such as Kindles and Nooks are allowed under the BYOD initiative (assuming the BYOD Agreement Form has been signed and returned.) The times and situations during which they can be used for casual, self-selected readings are determined by individual classroom educators. You can speak with your child's educators for recommendations on e-reader use in school.

Is this information available online?

A copy of this letter and the Personal Device Usage Agreement have been posted on the school website.

Red Deer Catholic Regional Schools

5530 - 42A Avenue	Telephone: (403) 347-7830
Red Deer, AB, T4N 3A8	Telecopieur / Fax: (403) 343-9285

Personal Device Usage Agreement

Any student wishing to bring their wireless Personal Electronic Devices (PEDs) to the Red Deer Catholic Schools must consent to the following agreement.

Red Deer Catholic Regional Schools does not guarantee the privacy or security of any item stored on or transmitted by any wireless PEDs.

The Parent and Student acknowledges that the wireless PEDs may inadvertently or willfully connect to the cellular network or outside wireless access points through an unsecured connection, which may or may not result in substantial data charges. The Parent and Student acknowledge that this will result in unauthorized, unfiltered access through these external connections while on school premises. Red Deer Catholic Regional Schools are not financially responsible for any downloaded applications purchased by students, data plan overages, or charges associated with texting/multimedia packages through any service provider. Teachers are not permitted to require students to download applications that are not free to the user.

Red Deer Catholic Regional Schools is not responsible for any loss, theft, or damage sustained to wireless PEDs.

A wireless PED can be connected to the Red Deer Catholic Regional School's network to access the internet under the following conditions:

- Use of the wireless PEDs must adhere to the Red Deer Catholic Regional Schools Administrative Procedure No. 114 Use of Cell Phones and Personal Electronic Devices (PEDs) in Schools and Student Acceptable Use of Internet/E-Mail Agreement (Form 33).

- The students must supply all necessary hardware/software to connect to Red Deer Catholic Regional Schools' wireless network.

- A student who brings their wireless PEDs to school is personally responsible for the equipment as well as all security, maintenance, and repair.

- Red Deer Catholic Regional Schools' Technology department will not service, repair or give support to any equipment not belonging to Red Deer Catholic Regional Schools. No internal components belonging to Red Deer Catholic Regional Schools' shall be placed in any wireless PEDs, whether as enhancements, upgrades, or replacements.

- Software residing on the wireless PEDs must be personally owned. If such software interferes with the Red Deer Catholic Regional Schools' software or hardware, this may result in a loss of wireless access privilege.

- The PEDs will not be connected to the Red Deer Catholic Regional Schools' wired network.

As it relates to wireless PEDs used in Red Deer Catholic Regional Schools' facilities, the Red Deer Catholic Regional Schools reserve the right to:

- Monitor all activity.

- Make determinations on whether specific uses of the wireless PEDs are consistent with Administrative Procedure No. 114, Use of Cell Phones and Personal Electronic Devices (PEDs) in Schools and Student Acceptable Use of Internet/E-Mail Agreement (Form 33).

- Deem what is appropriate.

- Remove the user's access to the network and suspend the right to use the wireless PEDs in Administrative Procedure No. 114, Use of Cell Phones and Personal Electronic Devices (PEDs) in Schools and Student Acceptable Use of Internet/E-Mail Agreement (Form 33) or violating the terms of this agreement.

I have read and consent to the above information. I am requesting that my wireless PEDs be granted wireless access to the Red Deer Catholic Regional Schools' wireless network. I also agree to hold my child accountable to the proper use of any personal electronic device and to be supportive of the school should my child violate the personal electronic device or technology acceptable use policies. (Complete the following information and return this form to the office.)

_____   _____   _____

Student Signature   Print Name   Date

_____   _____   _____

Parent Signature   Print Name   Date

If you have any questions or concerns, please phone or email Mr. Brehaut (tbrehaut@rdcrd.ab.ca), Mrs. Groenen (cgroenen@rdcrd.ab.ca), or Mr. Maschio (pmaschio@rdcrd.ab.ca).

Please refer to Administrative Procedure No. 114, Use of Cell Phones and Personal Electronic Devices (PEDs) in Schools (http://rdcrd.ab.ca/policy.html) and Student Acceptable Use of Internet/E-Mail Agreement (Form 33) (http://rdcrd.ab.ca/forms.html).