PRINCE ALBERT ROMAN CATHOLIC SEPARATE SCHOOL DIVISION NO. 6

POLICY ITEM: Information Technology Acceptable Use	**CODE: CN**
LEGAL STATUS: BOARD MOTION #17.14, #110.15	**DATE APPROVED: 27 Jan 2014, 11 May 2015**

Background: The Prince Albert Catholic School Division recognizes the importance and value of information technology for educational and administrative use. Information Technology (IT) is defined as hardware, software, and data as they pertain to the use of computers and other electronic devices to create, use, transmit, and store information.

POLICY: **The Board of Education directs the Director of Education to ensure the Information Technology Acceptable Use Policy is used to enhance teaching and learning and support program delivery based on the prescribed provincial curricula. The use of information technology will align with and expand upon the Ministry of Education CommunityNet Acceptable Use Policy. All users of the Prince Albert Roman Catholic Separate School Division Information Technology infrastructure are expected to use such systems in a legal, ethical, collegial, and non-destructive manner consistent with a spirit of respect and in accordance with the policies and procedures of Prince Albert Catholic School Division and within the laws of Saskatchewan and Canada.**

Guidelines:

1. All staff, administration, and trustees will use the school division technology for educational purposes and for the business and administrative functions directly in support of the school division's operations and abide by the Information Technology Acceptable Use Policy.
2. All students who enroll within the Prince Albert Catholic School Division will abide by the Information Technology Acceptable Use Policy. Parents/guardians will be informed and provide consent.
3. All non-employees granted temporary access to the school division technology infrastructure will abide by the Information Technology Acceptable Use Policy.
4. Usage of Prince Albert Catholic School Division information technology infrastructure will be limited to usage defined under Acceptable Use, Incidental Use, and Unacceptable Use (Appendix A).
5. The Director of Education will direct the technology department in monitoring of all aspects of technology use as required.
6. The IT department will have access to all stored data to help ensure a safe, secure and reliable information technology infrastructure subject to legal restriction regarding access to personal information.
7. The IT department will maintain strict confidentiality with regards to the authority granted with all aspects of technology.

8. All users will adhere to security procedures and protocols established for each user group.
9. All use of information technology will follow the letter and spirit of relevant licensing and copyright agreements.

Procedures:

1. All division employees will have access to the internet through the division's network.
2. Each employee will sign an Information Technology Acceptable Use Agreement as a condition of employment with the school division. The agreement will be kept in the personnel file.
3. Student use of the information technology infrastructure will be under the direction of the school principal working with staff to ensure the onsite supervision of students using the infrastructure.
4. The Elementary Student Information Technology Acceptable Use Agreement will be signed by the student and his/her parent(s)/guardian(s) upon registering with the school/school division. Confirmation of the signed agreement will be noted in the Student Data System.
5. The Secondary Student Information Technology Acceptable Use Agreement will be signed by the student (and his/her parent(s)/guardian(s) if under the age of 16) upon registering with the school/school division. Confirmation of the signed agreement will be noted in the Student Data System.
6. Students will be taught age-appropriate protocols regarding personal safety, infrastructure security, and acceptable/unacceptable use.
7. The non-employee Information Technology Acceptable Use Agreement will be agreed upon by individuals, from time to time, granted access to the school division for a specific purpose.
8. Employee failure to comply with the acceptable use agreement will be handled in accordance with division procedures and/or the Code of Ethics governing the conduct of professional and support staff.
9. Student failure to comply with the acceptable use agreement will be dealt with in accordance to the school's supervision and discipline policies.
10. Non-compliance with acceptable use agreements by staff or students may, depending on the severity of the situation, result in: suspension or cancellation of user privileges, request of payment for damages or repairs, suspension, expulsion, exclusion, or termination of employment, criminal or civil liability under applicable laws.
11. The Information Technology department may monitor users of Prince Albert Catholic School Division information technology infrastructure. Under the direction of the Director of Education, the IT Manager reserves the right to monitor and review all aspects of technology use when required. This includes, but is not limited to, internet and user created files. An individual search will be conducted if there is reasonable suspicion that a user has violated the law or the school/division's procedures. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation and will occur when the Director of Education deems necessary.
12.

13. To help ensure a safe, secure and reliable information technology infrastructure, IT personnel must perform maintenance, upgrades and auditing functions on all infrastructure devices thus requiring appropriate access to these devices, including access to stored data. Agreement to use school division infrastructure technology, as identified in acceptable use policies, constitutes access and is subject to legal restriction regarding access to personal information.
14. All records in the possession or under the control of the school division, including electronic records, are subject to *The Local Authority Freedom of Information and Protection of Privacy Act.*
15. Electronic records are subject to school division records management administrative policies as well as *Records Retention and Disposal Guide for Saskatchewan School Divisions.*
16. Employees who require access to computer systems in order to perform the duties of their role will be assigned usernames and passwords and follow the school division security protocols and acceptable use guidelines.
17. Website development and social networks will abide by the school division protocols and procedures.
18. Employees will not attempt to gain unauthorized access to information or facilities.
19. Employees permitted to use remote access to aspects of IT infrastructure are to ensure access is not gained by non-employees.
20. All computer hardware and software in use is purchased by the school division under academic licenses. Software must be used legally in accordance with relevant licensing and copyright agreements. Software that is not purchased by the Prince Albert Catholic School Division cannot be used in any capacity within the school division.
21. The Division makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the division network will be error-free or without defect. The Division will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The Division is not responsible for the accuracy or quality of the information obtained through or stored on the system. The Division will not be responsible for financial obligations arising through the unauthorized use of the system.

The usage of Prince Albert Catholic School Division Information Technology infrastructure falls under the categories of acceptable, incidental, and unacceptable. Acceptable use standards within the school division apply to all students, staff, trustees, and non-employees such as interns, presenters and other guests that have authorized access to the school division network.

The rules set out in the policy, including this appendix, provide general guidance and examples of acceptable or prohibited uses are for illustrative purposes and should not be construed as being exhaustive of unacceptable use. Employees who have questions as to whether a particular activity or use is acceptable should seek further guidance from the Director of Education or designate.

Acceptable Use

Acceptable uses are those activities that are required to conduct the business of education. They help fulfill mandates set forth by the school division and the Ministry. Any application that is used in the delivery of services by education partners which does not disproportionately consume available resources or compromise educational objectives is considered an acceptable use.

Incidental Use

Incidental uses are those that are neither explicitly permitted nor explicitly denied.

Incidental use may refer to the use of technology for private purposes. Such usage must adhere to the expectations that are set out in this policy.

Employees shall comply with the following incidental use rules of school division information technology infrastructure:

a) Incidental use must not interfere with the employee's work or the work of others.

b) Employees shall restrict personal communications during school/office hours to pressing matters only and such communications shall be brief.

c) Employees may not use their school division email address to post personal communications.

Unacceptable Use

Unacceptable use impedes the work of others and may damage or compromise school division information technology infrastructure, intentionally or unintentionally. This includes any use that significantly interferes with, or is incompatible with, the educational environment and the duties of employment, or any use that exposes the Board to significant cost or risk liability.

Unacceptable uses of the information technology infrastructure include but are not limited to:

a) Unauthorized release of information

1) Giving out personal information about another person, including home address and phone number.

2) Posting student picture, information on the internet without following protocol and permission from the Director or designate.

3) Providing internal information to outside parties.

4) Providing confidential information about the Board, or its operations, to outside parties.

b) Unauthorized personal use

1) Personal business or commercial or for-profit purposes.

2) Product advertisement or political lobbying including the sending of junk mail or other advertised material.

c) Misuse of passwords

1) Revealing a password to any person.

2) Attempting to discover another user's password.

3) Circumventing user authentication or security of any host, network or account.

4) Misrepresenting other users on the network.

d) Unauthorized use

1) Intentionally modifying hardware, software, files, mailbox, webpage and other data or passwords belonging to other users.

2) Unauthorized installation of any software (including shareware and freeware) and hardware.

3) Malicious use of the computer system to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system.

4) Making unauthorized entry to other computational, informational or communications devices or resources.

5) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.)

6) Effecting security breaches or disruptions of network communication including but not limited to accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

7) Allowing use of a user account by an unauthorized party including family members and friends.

e) Improper, objectionable or unethical actions

1) Creating or circulating hate mail, chain letters, harassment, discriminatory remarks and other antisocial behaviours.
2) Any unauthorized access, manipulation or modifications to the school division website.
3) Using the services in a malicious, threatening or obscene manner.
4) Use of profanity, obscenity, racist terms, or other language that may be offensive to another user.
5) Sending forged or anonymous email or postings.
6) Reposting a message that was sent privately without permission from the sender.

   7) Dispersing data proprietary to Prince Albert Roman Catholic School Division No. 6.
   8) Any form of harassment, including bullying, via any electronic means or through social networking sites whether through language, frequency or size of messages.
   9) Using school division resources for any activities that are offensive or perceived to be offensive to others, posting false or defamatory information about a person or organization.
   10) Transmission of inappropriate jokes or attachments, chain letters or spamming.
   11) Accessing electronically collected and stored information for personal use (e.g., student or employee personal contact information).

f) Misuse of copyright on licensing agreements

   1) Downloading, copying, otherwise duplicating and/or distributing copyrighted materials without the specific written permission of the copyright owner, except when permitted for educational purposes.

   2) Installation or distribution of products that are not appropriately licensed for use by the school division.

g) Prohibited use

   1) The network shall not be used in a deliberate manner that might disrupt the use of the network by others. Network bandwidth must be used in a manner that preserves bandwidth for educational purposes.

   2) Users shall not move, change, alter or add to the physical configuration of the school division's computers, servers, network hardware, cabling, printers and any associated peripherals. Only system approved standard hardware and software configured and installed by the IT Department is allowed to run on school division networks.

   3) Users shall not install software, including backgrounds or screen savers that would change the configuration of the computer system.

   4) Users shall not play web based games unless they are authorized to do so.

h) Illegal use

   1) Use of the IT infrastructure to access, process or store material that is prohibited (e.g., pornography), that advocates illegal acts, or that advocates violence or discrimination against other people.

   2) Use of the IT infrastructure for any criminal activity that can be punished under law.