HOLY FAMILY ROMAN CATHOLIC SEPARATE SCHOOL DIVISION NO. 140

OPERATIONS AND PROCEDURES

CATEGORY: SCHOOL OPERATIONS

TITLE: DIGITAL CITIZENSHIP

CODE: 5164 Digital Legal Responsibilities

Reference Matrix	
Education Act (1995)	Sections 85, 87, 108, 109, 175, 177, 231
Other Related Acts	Criminal Code; Copyright Act; *Local Authority Freedom of Information and Protection of Privacy(LAFOIP)*
Holy Family Related Procedures	OP 5163 Digital Access OP 5165 Digital Communication
Holy Family Related Manuals	
Resources (Ministry, SSBA, SCSBA, etc.)	Digital Citizenship Education in Saskatchewan Schools, 2015, Dr. Alec Couros-Information and Technology Coordinator at U of R.
Date Reviewed	August 21, 2016

Background:

In our connected world, there are specific legal responsibilities that students and staff must adhere to with regards to their actions in online settings. These legal responsibilities include, but are not limited to, issues such as fair dealing with copyright materials, illegal access to restricted materials (e.g. hacking), protection of one's own and others' digital identity, theft of digital materials, posting illicit and/or inappropriate information, and participating in online harassment or bullying. Holy Family is committed to ensuring that students and staff are equipped with the knowledge and understanding to act in appropriate and ethical ways with respect to digital law.

For the purpose of all Digital Citizenship Operational Procedures the term "users" includes all Holy Family administrators, teachers, staff, and students, as well as guests accessing the Holy Family network.

Procedures:

1. General Guidelines

1.1. Users will employ technology in a way that supports a positive learning environment, and in accordance with all associated laws. Reference OP 5163 Digital Access for signed agreements.

2. Illegal Activities

2.1. Users will not attempt to gain unauthorized access to the Division network or to any other computer system through the Division network. This includes attempting to login through another person's account or accessing another person's files.

2.2. Users will not make deliberate attempts to disrupt the computer system performance or to destroy data by spreading computer viruses or by any other means.

2.3. Users will not use the Division network to engage in any other illegal act as defined by law.

3. Network Monitoring

3.1. The computer network is owned by the Board, and the Board reserves the right to access the contents of all files stored on the network as well as all messages transmitted through its computer network.

3.2. The Board keeps and reserves the right to monitor logs of usage of school division equipment, whether it is used inside or outside the school. These logs may reveal information such as:

3.2.1. which internet servers and sites have been accessed by employees;

3.2.2. the email addresses of those with whom employees have communicated;

3.2.3. the content of communications including emails and instant messages.

3.3. Except as otherwise provided for in this policy, the Board:

3.3.1. will not engage in real-time surveillance of network or equipment usage;

3.3.2. will not disclose any logged, or otherwise collected, information to a third party except under compulsion of law.

3.4. Surveillance and disclosure by the Board may take place in the following circumstances:

3.4.1. in the case of a specific allegation of misconduct, the Director or designate may authorize access to such information when investigating the allegation;

3.4.2. when the Computer/Networking Support Technologist cannot avoid accessing such information in the course of fixing a problem.

3.5. In cases where information is accessed, any individuals affected will be informed and information will be disclosed no wider than is absolutely necessary.

4. Copyright Infringement and Plagiarism

4.1. All hardware and software in use is purchased under academic licenses: no commercial activity of any kind will be carried out on Division networks or Division equipment. (*LAFOIP*)

4.2. Software must only be used in legal ways in accordance with both the letter and spirit of relevant licensing and copyright agreements. (*LAFOIP*)

4.3. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure of acceptable use of a particular work, they should request permission from the copyright owner. (*Copyright Act*)

4.4. Users will not plagiarize works that they find on the Internet. Plagiarism includes taking the ideas or writings of others and presenting them as if they were original to the user.

5. Inappropriate Access to Material

5.1. Users will not use the Division's network to access material that is profane or obscene (including pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). For students, a special exception may be made for hate literature if the purpose of such access is to conduct research and the access is approved by both the teacher and the parent. Division employees may access the above material only in the context of legitimate research.

5.2. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access in the manner specified by their school. This will protect users against allegations that they have intentionally violated this protocol.

6. Electronic Intellectual Property Rights

6.1. Students shall retain all rights to work they create using the Division network or Division equipment.

6.2. As agents of the Division, employees shall have limited rights to work they create using the Division network of Division equipment. The Division shall retain the right to use any product created for its use by an employee even at such time as the author is no longer an employee of the Division.

7. In the event that cyber bullying is suspected or alleged, staff should refer to OP 5165 Digital Communication.

8. In the event that sexting is suspected or alleged, staff should refer to OP 5165 Digital Communication.

9. Disclaimer of Liability

9.1. The Division shall not be liable for users' inappropriate use of electronic resources, violations of copyright restrictions or other laws, users' mistakes or negligence, or costs incurred by users. The Division shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.