HOLY FAMILY ROMAN CATHOLIC SEPARATE SCHOOL DIVISION NO. 140

OPERATIONS AND PROCEDURES

CATEGORY: SCHOOL OPERATIONS

TITLE: DIGITAL CITIZENSHIP

CODE: 5168 Digital Safety and Security

Reference Matrix	
Education Act (1995)	Sections 85, 87, 108, 109, 175, 177, 231
Other Related Acts	
Holy Family Related Procedures	OP 5163 Digital Access
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:

Digital Safety and Security relates to the strategies and precautions that should be taken to ensure online security; particularly with reference to the protection of data against viruses, hacking, and device failure.

Holy Family believes that, with the assistance of the Division's Computer/Networking Support Technologist, students and staff have an individual responsibility to behave proactively to protect the security and safety of hardware, software, data, and passwords; doing so will ensure that the entire school division is less at risk for viruses, hackers, and potential loss of data.

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. Computer/Networking Support Technologist (CNST) Responsibilities

    1.1. Security / Protection of Student and Staff Data:

1.1.1. Each of the school's servers will be backed up to an external location on a nightly basis.

1.2. Personal Electronic Devices (PEDs) Connected to the Division Network

1.2.1. A password protected Wi-Fi network will be available as:

1.2.1.1. Private – for all Holy Family owned devices: passwords for the private network will be stored at each school with the Principal or designate, as well as with the CNST

1.2.1.2. Staff – for PEDs of Division employees: login and passwords will be the same as the staff login information for the Division network

1.2.1.3. Student – for PEDs of all students currently registered in the Division: login and passwords will be the same as the student login information for the Division network

1.2.1.4. Guest – for visitors to Holy Family wishing to access the Wi-Fi network: passwords for the guest network will be stored at each school with the Principal or designate, as well as with the CNST

1.3. Network Password Schedules

1.3.1. Staff - password is set by staff members and must be 8 characters in length, containing at minimum 1 number and 1 capital letter for security reasons.

1.3.1.1. Passwords are set to expire every 90 days.

1.3.2. Students – passwords are set by students and are to be 4 characters in length, containing 1 number; passwords may be reset by students as necessary.

1.4. Antivirus and Spyware Suppression

1.4.1. Each server and CNST approved school owned device as deemed appropriate by CNST is to have an antivirus program installed in an effort to reduce the overall likeliness of being infected with a virus.

1.5. Firewalls

1.5.1. Each school has its own firewall in order to filter and protect the school from unwanted digital intruders;

1.5.2. Firewalls may also be used to route and prioritize network traffic as determined by CNST.

1.6. Inventory of Technology

1.6.1. All items that are managed by the CNST department are to be maintained in an up-to-date inventory database. The database will house the following information: make, model, serial number, location of the asset, and assigned user (where applicable).

1.7. Crisis Preparation

1.7.1. In the event of a catastrophic issue with Holy Family's network, all data stored in the cloud will be retrievable; data stored on local devices or Division drives and servers may be lost. Therefore, device data should be backed up accordingly.

1.8. Disposal of Holy Family Hardware

1.8.1. The CNST will ensure that data on devices has been erased/ destroyed/disposed of correctly.

1.8.2. All hardware is to be disposed of by the CNST department through a recognized recycling provider within the province.

1.8.3. In order to qualify as a recognized recycling provider, the provider must provide a certificate of collection and destruction of data.

1.9. Configuration Testing

1.9.1. Configuration will be monitored by CNST and addressed as necessary.

1.10. Monitoring

1.10.1. Monitoring of all technology infrastructure systems is intended to occur annually; there will be a five (5) year plan for updating Holy Family's infrastructure as necessary, including, but not limited to: hardware (computers, tablets, etc.), software, servers, networks, apps, switches, firewalls, and surge protection.

2. Student and Staff Responsibilities

2.1. Securing / Storage of data

2.1.1. Users are expected to store all school related material on the Division's cloud network.

2.1.2. Material created by Division staff for the purpose of carrying out work-related duties is the property of the Division; therefore, storage of such material is not permitted on personal devices, drives, etc.

2.2. Passwords

2.2.1. Students are not to share network passwords with any other student; students may share passwords with parent(s)/guardian(s) or with staff members who supervise or are directly responsible for their educational programming.

2.2.2. Division employees are not to share network passwords with anyone except those employees who directly supervise their work.

2.2.3. Division employees are expected to change passwords as scheduled by the CNST department to help increase security.

2.3. Securing of Personal Electronic Devices (PEDs)

2.3.1. Users should refer to OP 5163 Digital Access.