ADMINISTRATIVE PROCEDURE NO. 116

INFORMATION SECURITY

Background

The Division recognizes the responsibility to provide a Christ-centered, safe and caring school learning environment for students that require the support and assistance of all members of the community. To ensure the security and privacy of student information, the Division is required to implement Division security procedures as these relate to, but not limited to, students, staff, volunteers, contractors, vendors and agents working within the Division. The purpose of this administrative procedure is to define standards for protecting Division information especially sensitive and personal information, from unauthorized collection, use, disclosure, retention or destruction.

Information means all information in the custody or under the control of the Division whether electronic or other recorded format, and includes administrative, financial, personal, and student information, and the information about those who interact or communicate with the Division. This includes information found in student records and electronic records.

All information must be maintained in confidence and disclosed only if authorized by regulation or law including, but not limited to, the School Act, the Freedom of Information and Protection of Privacy Act, the Child Welfare Act, and the Income Tax Act.
RDCRD staff has access to sensitive personal information belonging to staff and students. This information must only be used in the performance of their RDCRD duties and responsibilities.

Procedures

The Division recognizes its obligation to provide appropriate levels for protecting sensitive and personal information.

1. The Superintendent is accountable to ensure the Division is undertaking a due diligence process with information security.

2. The principal of each school is accountable for compliance of information security procedures.

3. The implementation and support of protecting information applies to, but not limited to, all Division employees, volunteers, contractors, vendors and agents who are able to connect to the Division network.

4. The Division shall advise the Freedom of Information and Protection of Privacy Commissions office and Alberta Education of any actual or potential breach of privacy or security, as soon as the Division becomes aware of such breach, including a known threat that has not yet resulted in a breach, which may affect information about Division employees, students or outside vendors.

5. Sensitive or confidential information must be stored in a secure location with restricted access. The nature of security measures must be adequate and appropriate for the sensitivity of the information to be protected. Security measures must be taken when transporting or transferring sensitive or confidential information, for example, emailing or faxing confidential information.

6. Portable devices utilized outside the Division must use the Division portal to access and save data. Division staff must not download, open or save personal information on portable devices. Any portable devices must have a password to restrict access.

7. It is the responsibility of Division employees, volunteers, contractors, vendors and agents with remote access privileges to the Division's corporate network to ensure their remote access connection is secure. At no time should any Division employee provide their login or email password to anyone, not even family members.

8. All email that is sent or received via Division emails systems, whether personal or work related, is in the custody of and under the control of the Division for records management, security and the Freedom of Information and Protection of Privacy (FOIP) purposes. Personal email messages may be included in Division responses to FOIP access requests or privacy complaints.

9. Risk assessments, which may include threat/risk assessment, privacy impact assessments or other assessments as necessary, shall be conducted on any new business process, system application or service, if it involves the collection, use or disclosure of personal or otherwise sensitive personal information.

10. Appropriate security measures must be taken when using all work areas and devices to ensure confidentiality, integrity and availability of sensitive information.

11. All system passwords must be changed yearly. Passwords must not be inserted into email messages or other forms of electronic communication.

12. In the event that Division data or applications are hosted, managed or supported by Application Service Providers (ASPs), a binding contract with the ASP must fully specify the privacy and security measures to be employed to ensure that the ASP services provide a level of protection equivalent to that provided by the Division.

13. All wireless infrastructure devices that reside at a Division site and connect to a Division network must be installed, supported and maintained by the Division's IT Department, use Division approved authentication protocols and infrastructure, use Division approved encryption protocols.