INFORMATION SECURITY

Background

The purpose of this procedure is to define standards for protecting the Division's information, especially sensitive and personal information, from unauthorized collection, use, disclosure, retention, or destruction.

Definitions

Division

The term *Division* refers to Battle River Regional Division No. 31.

Employee

The term *Employee* refers to the meaning given in the Freedom of Information and Protection of Privacy Act and includes employees, contractors, volunteers, and others providing services to, or on behalf of, the Division.

End User

The term *End User* refers to any employee, as defined, and students of the Division.

Information

The term *information* refers to all information in the custody or under the control of the Division, whether in electronic or other format, and includes administrative, financial, personal and student information (whether the student is enrolled with the Division or not), and information about those who interact or communicate with the Division.

Mobile Device

The term *mobile device* refers to any portable electronic device capable of storing information (e.g. laptop, PDA(personal digital assistant), cell phone, removable drive, any mobile or portable computing or storage device such as gaming devices).

Offensive

The term *offensive* refers to any comment that is offensive in nature about race, gender, hair color, disabilities, age, sexual orientation, religious belief, religious practice, political belief, or national origin; as well as that which would engage in public incitement, willful promotion of hatred, pyramid selling, mischief in relation to information, fraud, defamatory libel, obscenity, pornography, harassment, stalking and uttering threats or any such activity that constitutes a criminal offence.

Personal Information

The term *personal information* refers to recorded information about an identifiable individual, including

- the individual's name, home or business address, or home or business telephone number;
- the individual's race, national or ethnic origin, color, or religious or political beliefs, or associations;
- the individual's age, sex, marital status or family status;
- an indentifying number, symbol or other particular assigned to the individual;
- information about the individual's health and health care history including information about a physical or mental disability;
- information about the individual's educational, financial, employment or criminal history, including criminal records;
- anyone else's opinions about the individual;
- the individual's personal views or opinions, except if they are about someone else; and
- student records.

Risk

The term *risk* refers to any factor that could be detrimental to the confidentiality, availability, integrity, or privacy of information in the custody of or under the control of the Division.

Workstation

The term *workstation* refers to laptops, desktops, PDAs (personal digital assistants), tablets and any other electronic devices containing or accessing Division information, including authorized home workstations accessing the Divisions' network.

Accountability

The Superintendent of Schools is accountable, in general, for the Division's compliance with this procedure and for maintaining and updating this procedure.

The supervisor of a department operated by the Division is accountable for that department's compliance with this procedure.

The principal of a school operated by the Division is accountable for that school's compliance with this procedure.

Scope

This procedure applies to all the Division's employees, contractors, vendors and agents with a Division-owned or personally owned computer or workstation used to connect to the Division network.

This procedure applies to remote access connections used to do work on behalf of the Division, including reading or sending email and viewing intranet web resources.

This procedure applies to anyone using the Division's information including, but not limited to, employees, agents, appointees, consultants, contractors, persons on secondment, volunteers, practicum students, student teachers, exchange teachers, and students.

Enforcement

Any employee found to have violated this procedure may be subject to disciplinary action.

Procedures

1. INFORMATION SECURITY PRINCIPLES

    1.1. Only authorized persons may have access to information.

    1.2. 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.

    1.3. Only authorized persons may use, disclose, take, alter, copy, interfere with, or destroy information, and must do so according to law and the Division's Records Management Procedure and Directives and Guidelines.

    1.4. Each person using the Division's information at a Division location or otherwise, is responsible for the management and safekeeping of information under their control by ensuring that there is adequate security to prevent unauthorized access, collection, use, disclosure or disposal of information.

    1.5. Security measures must be used for;
    - documented information;
    - electronic information;
    - access to recorded messages, voice mail and telephone answering machines; and
    - access to and within buildings.

    1.6. The nature of security measures must be adequate and appropriate for the sensitivity of the information to be protected.

1.7. Employees, who will be accessing the Division's network, will be required to read and sign the documents Confidentiality Undertaking and Employee Acceptable Use Agreement Form to ensure that they understand their information security obligations.

2. EMAIL USE

2.1. The Division email shall not be used to create, reproduce, distribute or otherwise transmit any information/message that is considered offensive by the Division.

2.2. Reasonable, limited use of Division resources for personal emails is acceptable.

2.3. Employees who receive any emails with offensive content, from any Division employee, should report the matter to their supervisor immediately

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

3. CELLULAR TELEPHONES, EMAILS AND FAXES

3.1. Caution must be used when conveying personal or confidential information over insecure technologies such as cell phones, email or speakerphone.

3.2. When personal or confidential information must be conveyed by email it should be encrypted and/or secured with a password before being attached and sent. If scanning the document to send by email do not send it direct, scan to the network, secure the document then send it.

3.3. It is understood that some external parties have rules in places that requires them to send personal information via fax. Battle River employees will not send personal or confidential information via fax unless required by that third party.

4. SECURE STORAGE OF INFORMATION

4.1. Personal, sensitive or confidential information must not be left unattended on desks, in offices or in areas where unauthorized persons or members of the public may see or have access to them unless the desk, office or area can be secured from unauthorized access (e.g. placing files in a locked drawer or locking the office/area).

4.2. Personal, sensitive or confidential information must be stored in a secure location with restricted access, such as secure electronic storage, a locked room, or a locked filing cabinet.

4.3. Security measures must be appropriate for the sensitivity of the information being stored regardless of the physical or electronic medium on which it is stored.

4.4. When transporting or transferring personal, sensitive or confidential information care must be taken so that it reaches its intended destination intact and without unauthorized access or disclosure. A record of and a copy of, any information that which is to be transferred or stored on a mobile device, must be kept on the Division's network. If the mobile device is ever lost or stolen, the Division is required by FOIP legislation to be able to identify the information that has been compromised so that all affected persons can be notified as to the extent of their information that has been lost.

4.5. The Division's Technology Department will employ full disk encryption on Division mobile devices determined to be at risk. It is the end users' responsibility to identify, to the Technology Department, that they have a mobile device that is at risk and requires encryption.

4.6. All keys used for encryption and decryption must meet complexity requirements described in the passwords section of this procedure.

5. LOSS OF PERSONAL INFORMATION

5.1. In the event of a loss or suspected breach of personal information, whether contained in a paper file or on a mobile device, the Division process shall be followed.

5.1.1. Contact the immediate supervisor/school administrator and report the loss.

5.1.2. The supervisor/school administrator is then responsible to report the loss immediately to:

a. the Division's FOIP Coordinator, and;
b. the Directory of Technology if the loss included physical property of the Division or the physical property of the person which had been configured to connect to the Division network and/or contained Division information (e.g. laptop, blackberry, USB drive).

5.1.3. The Division's FOIP Coordinator will provide support and direction in regards to the loss/breach.

6. DISPOSAL OF INFORMATION

6.1. Any information that is no longer required, and the retention of which is not regulated by law, may only be destroyed in accordance with the Division's Records Management Procedure.

7. PRIVACY COMPLAINTS

7.1. All privacy complaints must be forwarded to the Division's FOIP Coordinator.

8. PASSWORDS

8.1. System-level passwords should be changed regularly.

8.2. User-level passwords (e.g. email, web, desktop computer) should be changed annually.

8.3. Application specific passwords must be changed as required by the application settings, e.g. Financial System.

8.4. Passwords shall have the following characteristics and are the responsibility of the end user:

- be comprised of a combination of at least 6 alpha and numeric characters;
- not be based on personal information;
- contain at least one number and one character; and
- have both upper and lowercase.

8.5. Passwords should not be inserted into email messages or other forms of electronic communication.

8.6. Passwords must never be written down, stored on-line unencrypted, or shared.

9. DIVISON NETWORK CONTROLS

9.1. Technology is a finite resource and is to be used in appropriate and ethical ways. Any use that could disrupt the use of the network by other users constitutes unacceptable use.

9.2. End users are subject to all policies and practices of the Division and individual schools/sites as related to technology, property or conduct. In particular, end users are also expected to abide by Administrative Procedure #140 - Acceptable Use of the Wide Area Network and the Internet and Administrative Procedure #170 - Harassment-Free Work Environment.

9.3. End users will not attempt to circumvent any of the Division's computer security measures.

9.4. End users are responsible for the security of access (i.e. login and password) to their network resources. End users will not share their password with others, nor will they maintain an unsupervised login that compromises network security. End users are expected to regularly change passwords, never allowing another person to use their account. End users are responsible for problems caused by use of their login by other individuals.

9.5. Only equipment, purchased through or managed by the Division, may be physically connected to the wired network or used to access file or print services. Personally-owned devices shall be connected to the appropriate available wireless network.

9.6. Any external/portable storage device that is connected to a Division computer becomes part of that computer and the content becomes property of the Division and should be treated as such.

9.7. Storage space is for Division-related information only.

9.8. End users will not publish, on any publicly viewable location, personal information about students or other end users. Any such publishing must meet the Freedom of Information and Protection of Privacy guidelines.

9.9. When using material or intellectual property developed by another person, end users must always cite the source and, if required, request prior consent from the developer.

9.10. The Division has the right to review any material on user accounts and to monitor end users at any time. This includes, but is not limited to, email, internet history, and server use whether the material is stored within the Division or in the BRSD Google domain.

9.11. In order to avoid compromising the operation of the network through unacceptable use, end users will not initiate or participate in malicious activity directed against network resources or users; and will not use unauthorized personal programs or data-files (e.g. non-educational audio, video, or executable files).

9.12. The Division has taken reasonable precautions to ensure responsible use and to restrict access to offensive and questionable information. The Division cannot be held liable for unacceptable use.

9.13. It is the responsibility of any end users to report any offensive or inappropriate use to their supervisor, who will consult the Superintendent or designate.

9.14. Access entails responsibility. The ultimate responsibility for appropriately using technology rests in the hands of the end user.

10. REMOTE ACCESS

10.1. It is the responsibility of each of the Division's end users using remote access privileges to the Division's corporate network to ensure that their remote access connection is secure. End users are responsible for any data loss, or breach of data security, when accessing Division data using a remote tool that was not installed and/or approved by the BRSD Technology department.

11. MOBILE EMPLOYEE RESPONSIBILITY

11.1. This procedure applies to any mobile device issued by the Division or used for Division business, which contains stored information owned by the Division.

11.2. All employees shall be responsible in protecting mobile devices issued by the Division or storing Division information by providing security through passwords and screen lock-ups (e.g. password locks on cell phones that are accessing Division email).

11.3. Unless written approval has been obtained from the Division, databases, or portions thereof, that reside on the network at the Division shall not be downloaded or copied to mobile devices.

11.4. Mobile devices that contain confidential, personal, or sensitive information must use encryption or equally strong measures to protect the information while it is being stored. It is the end user's responsibility to either provide adequate encryption or to inform the Technology Department that the device requires encryption.

11.5. Upon replacement or retirement of a personal mobile device, it is the end users responsibility to securely clear all Division information from that device.

11.6. Upon voluntary or involuntary termination, it is the end users responsibility to securely clear all Division information from their personal mobile device.

11.7. All employees shall be aware that compliance with all applicable Division procedures and standards related to mobile devices is mandatory.

12. WORKSTATION SECURITY

12.1. End users must take into consideration the sensitivity of the information that they are accessing and must be responsible to minimize the possibility of unauthorized access. Appropriate measures must be taken to ensure the confidentiality, integrity and availability of all information and may include but are not restricted to:

- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access;
- Complying with all applicable password policies and procedures;
- Never installing unauthorized software on workstations;
- Complying with all applicable encryption requirements (see 4.4 and 11.4); and
- Storing all sensitive information on network servers, not local drives.

12.2. The Division will implement physical and technical safeguards for all workstations that access personal information. Appropriate measures may include but are not restricted to:

- Restricting physical access to workstation to only authorized personnel;
- Enabling group policies that implement security (e.g. a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected);
- Ensuring workstations are used for authorized business purposes only;
- Ensuring that anti-virus and anti-malware programs are running and up to date, where applicable; and
- If wireless network access is used, ensuring that access is secured using appropriate security measures and standards, such as WPA or a virtual private network (VPN).

13. GENERAL NETWORK ACCESS

13.1. When network service and access procedures are revised, end users will update practice/use as required.

13.2. All wireless infrastructure devices that reside at a Division site and connect to the Division network must:

- Be installed, supported, and maintained by an approved support team;
- Use Division approved authentication protocols and infrastructure;
- Use Division approved encryption protocols; and
- Not interfere with wireless access deployments maintained by other support organizations.

13.3. The Division makes no warranties of any kind for services provided.

13.4. The Division will not be responsible for any damages (e.g. loss of information, non-deliveries, mis-deliveries or service interruptions). Any work may be subject to loss. End users must ensure responsible use and transmission of information (e.g. saving, sending, storing).

14. RISK ASSESSMENT

14.1. Risk assessments, which may include threat, privacy impact 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.

14.2. Risk assessments can be conducted on any information system, including applications, servers and networks, and any process or procedure by which these systems are administered and/or maintained.

14.3. Any risks identified by the risk assessment shall be mitigated by reasonable means that are effective for the purpose.

14.4. Privacy impact assessments shall be reviewed by the FOIP Coordinator or designate.

14.5. Threat/risk assessments shall be reviewed by the Division's Assistant Superintendent of Business or designate.

14.6. End users are expected to cooperate fully with any risk assessment being conducted on systems, processes or services for which they are held accountable, and to assist in the development of any related risk mitigation plans or measures.

15. APPLICATION SERVICE PROVIDERS (ASPS)

15.1. In the event that Division information or applications are to be hosted by an ASP, an agreement with the ASP must 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 itself.

Reference: Freedom of Information and Protection of Privacy Act
School Act R.S.A. 2000, c.S-3, ss 23, 60(3)(c)
BRSD #31 Administrative Procedure #140 – Acceptable Use of the Wide Area Network and the Internet
BRSD #31 Administrative Procedure - Records Management