INFORMATION SECURITY

Background

The Division believes that standards for protecting information must be in place to provide a safe and caring work environment for all stakeholders that ensures their privacy. 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

Employee Refers to the meaning given in the Freedom of Information and Protection of Privacy (FOIP) Act and includes employees, school division trustees, contractors, consultants, temporary workers, volunteers, and others providing services to, or on behalf of, the Division.

End User Refers to any *Employee*, as defined, and students of the Division.

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 Refers to any portable electronic device capable of storing information (e.g. laptop, cell phone, removable drive, any mobile or portable computing or storage device such as gaming devices).

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 label, obscenity, pornography, harassment, stalking and uttering threats or any such activity that constitutes a criminal offence.

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, gender, marital status or family status;
- an identifying 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 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.

Vendor An individual who provides products or services to a business for a fee.

Workstation Refers to laptops, desktops, tablets and any other electronic devices containing or accessing Division information, including authorized home workstations accessing the Divisions' network.

Procedures

1. **Employee**

    1.1 An *Employee* who will be accessing the Division's network will be required to read and sign the following to ensure that they understand their information security obligations (forms referenced in AP 140):
        1.1.1 Confidentiality Undertaking form
        1.1.2 Technology (Internet/Network) Acceptable Use Agreement-Network User form (140-3)

2. **Student**

    2.1 A student who will be accessing the Division's network will be required to read and sign the following to ensure that they understand their information security obligations (form referenced in AP 140):
        2.1.1 Technology (Internet/Network) Acceptable Use Agreement-Students (K-12) form (140-1)

3. **Accountability**

    3.1 The Superintendent of Schools is accountable, in general, for the Division's compliance with this procedure and for maintaining and updating this procedure.
    3.2 The supervisor of a department operated by the Division is accountable for that department's compliance with this procedure.
    3.3 The principal of a school operated by the Division is accountable for that school's compliance with this procedure.

4. **Scope**

    4.1 This procedure applies to:
        4.1.1 all the Division's *Employees*, Contractors, *Vendors* with a Division-owned or personally owned computer or *Workstation* used to connect to the Division network;
        4.1.2 remote access connections used to do work on behalf of the Division, including reading or sending email and viewing intranet web resources; and
        4.1.3 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.

5. Information Security Principles

5.1 Only authorized persons may have access to information.

5.2 All information must be maintained in confidence and disclosed only if authorized by regulation or law, including, but not limited to, the *Education Act*, the *FOIP Act*, the *Child, Youth and Family Enhancement Act*, and the *Income Tax Act.*

5.3 Only authorized persons may use, disclose, take, alter, copy, interfere with, or destroy information, and must do so according to law and Administrative Procedure (AP) 142 "Records Management" and "*Appendix A - Records Management Retention, Disposition and Filing Guidelines".*

5.4 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.

5.5 Security measures must be used for:

5.5.1 documented information;

5.5.2 electronic information;

5.5.3 access to recorded messages, voicemail and phone answering machines; and

5.5.4 access to and within buildings.

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

6. Email Use

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

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

6.3 An *Employee* who receives any emails with *offensive* content from any Division *Employee* should report the matter to their supervisor immediately.

6.4 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 *FOIP Act* purposes. Personal email messages may be included in Division responses to FOIP access requests or privacy complaints.

6.5 Caution must be used when conveying personal or confidential information over insecure technologies such as email.

7. Faxes and Desktop Phones

7.1 Caution must be used when conveying personal or confidential information over insecure technologies such as fax or speakerphone.

7.2 It is understood that some external parties have rules in places that require them to send *Personal Information* via fax. An *Employee* will not send personal or confidential information via fax unless required by that third party.

8. Secure Storage of Information

8.1 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).

8.2 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.

8.3 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.

8.4 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 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.

8.5 The 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.

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

9. Loss of Personal Information

9.1 In the event of a loss or suspected breach of *Personal Information*, including information in a paper file or on a *Mobile Device*, contact the immediate supervisor/School Administrator(s) and report the loss.

9.2 The supervisor/School Administrator(s) is then responsible to report the loss immediately to:

9.2.1 the Division's FOIP Coordinator, who will provide support and direction in regards to the loss/breach; and

9.2.2 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, mobile device, USB drive).

10. Disposal of Information

10.1 Any information that is no longer required, and the retention of which is not regulated by law, may only be destroyed in accordance with AP 142 - Records Management.

11. Privacy Complaints

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

12. Passwords

12.1 System-level passwords should be changed regularly.

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

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

12.4 Passwords shall have the following characteristics and are the responsibility of the *End User*:

12.4.1 Unable to use the same 5 passwords you have used previously

12.4.2 be changed every 6 months

12.4.3 have a minimum length of 14 characters
12.4.4 contain characters from three of the following four categories:
- Uppercase characters
- Lowercase characters
- Base 10 digits (0 through 9)
- Non Alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/

12.5 Passwords should not be inserted into email messages or other forms of electronic communication.
12.6 Passwords must never be written down, stored on-line unencrypted, or shared.
12.7 It is mandatory that Google two factor authentication be utilized for any *Employee* that is using a BRSD Google account.

13. **Division Network Controls**

13.1 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.
13.2 *End Users*:
13.2.1 are subject to all policies and practices of the Division and individual schools/sites as related to technology, property or conduct;
13.2.2 are expected to abide by AP 140 - Technology (Internet/Network) Acceptable Use and AP 170 - Harassment-Free Work/School Environment;
13.2.3 will not attempt to circumvent any of the Division's computer security measures;
13.2.4 are responsible for the security of access (i.e. login and password) to network resources;
13.2.5 will not share their password with others;
13.2.6 will not maintain an unsupervised login that compromises network security;
13.2.7 are expected to regularly change passwords;
13.2.8 are to never allow another person to use their account;
13.2.9 are responsible for problems caused by use of their login by other individuals;
13.2.10 will not publish, on any publicly viewable location, *Personal Information* about students or other *End Users*. Any such publishing must meet FOIP guidelines;
13.2.11 when using material or intellectual property developed by another person, must always cite the source and, if required, request prior consent from the developer;
13.2.12 are responsible to report any *offensive* or inappropriate use to their supervisor, who will consult the Superintendent or designate;
13.2.13 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), in order to avoid compromising the operation of the network through unacceptable use.
13.3 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.
13.4 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.
13.5 Storage space is for Division-related *Information* only.
13.6 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.

13.7 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.

13.8 Access entails responsibility. The ultimate responsibility for appropriately using technology rests in the hands of the *End User*.

14. **Remote Access**

14.1 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 Division's Technology Department.

15. **Mobile Devices**

15.1 This procedure applies to any *Mobile Device* issued by the Division or used for Division business, which contains stored *Information* owned by the Division.

15.2 An *Employee* shall be responsible for protecting *Mobile Devices* that are either issued by the Division or are personally owned when storing Division *Information* by providing security through passwords and screen lock-ups (e.g. password locks on cell phones that are accessing Division email). This also includes *Employees* receiving stipends for personally owned cellular phones to conduct Division business.

15.3 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.

15.4 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.

15.5 Upon replacement or retirement of a personal *Mobile Device*, it is the *End User's* responsibility to securely clear all Division *Information* from that device.

15.6 Upon voluntary or involuntary termination, it is the *End Users* responsibility to securely clear all Division *Information* from their personal *Mobile Device*.

15.7 Caution must be used when conveying confidential or *Personal Information* over insecure technologies such as cell phones.

16. **Workstation Security**

16.1 *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:

- 16.1.1 Securing *Workstations* (screen lock or logout) prior to leaving area to prevent unauthorized access;
- 16.1.2 Complying with all applicable password policies and procedures;
- 16.1.3 Never installing unauthorized software on *Workstations*;
- 16.1.4 Complying with all applicable encryption requirements; and
- 16.1.5 Storing all sensitive *Information* on network servers, not local drives.

16.2 The Division will implement physical and technical safeguards for all *Workstations* that access *Personal Information*. Appropriate measures may include but are not restricted to:

16.2.1 Restricting physical access to a *Workstation* to only authorized personnel;

16.2.2 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);

16.2.3 Ensuring *Workstations* are used for authorized business purposes only;

16.2.4 Ensuring that anti-virus and anti-malware programs are running and up to date, where applicable; and

16.2.5 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).

17. **General Network Access**

17.1 When network service and access procedures are revised, *End Users* will update practice/use as required.

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

17.2.1 Be installed, supported, and maintained by an approved support team;

17.2.2 Use Division approved authentication protocols and infrastructure;

17.2.3 Use Division approved encryption protocols; and

17.2.4 Not interfere with wireless access deployments maintained by other support organizations.

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

17.4 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).

18. **Risk Assessments:**

18.1 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*;

18.2 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;

18.3 Any *Risks* identified shall be mitigated by reasonable means that are effective for the purpose;

18.4 Privacy impact assessments shall be reviewed by the FOIP Coordinator or designate;

18.5 Shall be reviewed by the Secretary-Treasurer or designate; and

18.6 *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.

19. Application Service Providers (ASPs)

19.1 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.

20. Enforcement

20.1 Any *End User* found to have violated this procedure may be subject to disciplinary action. For *Employees*, this may also include disciplinary action up to and including termination.

Reference: Freedom of Information and Protection of Privacy Act
Section 52, 53, 222, Education Act

Related APs:

Technology (Internet/Network) Acceptable Use	(140)
Records Management	(142)
Harassment-Free Work/School Environment	(170)

Forms: refer to AP 140 for applicable forms

Amended: June 2023