Administrative Procedure 192

INFORMATION SECURITY PROCEDURES

Background

The purpose of the information security procedure is to define standards for protecting Division information, especially sensitive and personal information, from unauthorized collection, use, disclosure, retention or destruction. All sensitive information that is retained or generated by Division staff must be held in a secure manner. Whether the information is in an electronic format or on paper the security of that information must be maintained. This applies to all Division employees, contractors, vendors, volunteers and agents with a Division-owned or personally-owned computer or workstation used to connect to the Division network. It also applies to remote access connections used to do work on behalf of the Division, including reading or sending email and viewing intranet web resources.

Definitions

1. *Division* means Black Gold School Division.

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

3. *Personal information* means recorded information about an identifiable individual, including:
   - 1.1 the individual's name, home or business address or home or business telephone number;
   - 1.2 the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;
   - 1.3 the individual's age, sex, marital status or family status;
   - 1.4 an identifying number, symbol or other particular assigned to the individual;
   - 1.5 the individual's fingerprints, blood type or inheritable characteristics;
   - 1.6 information about the individual's health and health care history, including information about a physical or mental disability;
   - 1.7 information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
   - 1.8 anyone else's opinions about the individual;
   - 1.9 the individual's personal views or opinions, except if they are about someone else; and
   - 1.10 student's record. (Refer to AP 320 – Student Records)

2. *Employee* has 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.

3. *Student information* means personal information about a student, whether enrolled with the Division or not, including information about any student contained in PASI. (Refer to AP 320 – Student Records)

4. *PASI* means the Provincial Approach to Student Information database an application and repository of student information maintained by Alberta Education.

5. *PASIprep* provides a user interface to manage and access the information within PASI. PASIprep is primarily used by Alberta Education users and school/authority users for PASI functionality that has not been integrated into the local Student Information System (SIS).

6. *Risk* means any factor that could be detrimental to the confidentiality, availability, integrity or privacy of information in the custody or control of Black Gold School Division.

Procedures

1. Enforcement

    1.1 Any employee found to have violated these procedures may be subject to disciplinary action, up to and including termination of employment.

2. Information Security Principles

    2.1 Only authorized persons may have access to information.

    2.2 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 Freedom of Information and Protection of Privacy Act, the Child Welfare Act, and the Income Tax Act.

    2.3 Only authorized persons may use, disclose, take, alter, copy, interfere with, or destroy information, and must do so according to law and Division records management standards, procedures, and practices.(Refer to AP 185 – Records and Information Management)

    2.4 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. (Refer to AP 185 – Appendix A – Records Retention Schedule)

    2.5 Security measures must be used for electronic information;

        2.5.1 Access to recorded messages, voice mail, telephone answering machines and security cameras; and access to and within buildings.

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

2.5.3 Employees will be provided with training and awareness materials as necessary to ensure that they understand their security obligations.

3. Cellular Telephones, E-mails and Faxes

3.1 Caution must be used when conveying confidential information over insecure technologies such as cellular telephones, e-mail and faxes.

4. Clean Desks

4.1 Records containing sensitive or confidential information must not be kept on desks or in places where unauthorized persons or members of the public may see or have access to them.

5. Secure Storage of Information

5.1 Sensitive or confidential information, including servers, must be stored in a secure location with restricted access, such as secure electronic storage, a locked room, or a locked filing cabinet. 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.

5.2 Care must be taken when transporting or transferring sensitive or confidential information so that it reaches its intended destination intact and without unauthorized access or disclosure.

5.3 Staff mobile devices must employ full disk encryption with an approved software encryption package. No Division data may exist on a laptop in cleartext.

5.4 All keys used for encryption and decryption must meet minimum complexity requirements described in section 13 of this procedure.

6. Disposal of Information

6.1 Any information that is no longer required for either administrative, educational, financial, legal or historical purposes, and the retention of which is not regulated by any provincial or federal law, may only be destroyed in accordance with records management procedures and practices. (Refer to AP 185 – Records and Information Management)

7. Privacy Complaints

7.1 All privacy complaints must be forwarded to the Freedom of Information and Protection of Privacy Coordinator, Associate Superintendent, Human Resources.

8. Remote Access

8.1 The Division takes no responsibility for any effect on a computer system that installing any remote client access software may result in. The choice to install this software and use an account is entirely at the discretion of the eligible staff member (generally teachers and office staff) and in no way should be construed as a condition of employment.

8.2 Access to the Division network resources through a BG-Remote Access account is restricted to the individual account holder. User ID's and passwords must not be

shared with any other person including spouses, children, other employees or non-employees.

8.3 The account holder, by applying for this account, accepts responsibility for all activities and actions resulting from use of the account.

8.4 It is the responsibility of each Division employee, contractor, vendor and agent with remote access privileges to the Division's corporate network to ensure that their remote access connection is as secure as the user's on-site connection to the Division.

8.5 At no time should any employee provide their login or email password to anyone, not even family members.

8.6 All hosts that are connected to the Division internal networks via remote access technologies must use a VPN (virtual private network) - based remote connection through RDP (remote desktop protocol) so no viruses can propagate automatically – any files copied from home to the server are scanned on the server, but it is strongly recommended that an antivirus program be enabled on non-Division computers.

8.7 Software installation and technical problem resolution on personal hardware used for remote access is the responsibility of the individual user. If you should seek support from a third party, you must ensure that your passwords remain completely confidential and are not shared.

8.8 Schools, departments or individuals who wish to implement non-standard Remote Access solutions to the Division private network must obtain prior approval from the Technology Department.

9. Email Use

9.1 The Division email system will not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any employee should report the matter to their supervisor immediately.

9.2 Reasonable, limited use of Division resources for personal email is acceptable, but non-work related email will be saved in a separate folder from work related email.

9.3 Division email will not be used for commercial use, product advertisement or political lobbying.

9.4 All email that is sent or received via Division email systems, 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 the Division responses to FOIP access requests or privacy complaints.

10. Mobile Employee Endpoint Responsibility

10.1 See Portable Technology Security – Administrative Procedure 141 – Portable Technology Security

10.2 This guideline applies to any Division mobile device, used by any employee.

10.3 Any staff device that is lost or stolen, must be reported immediately to the FOIP Coordinator and the IT Manager.

11. Risk Assessment

11.1 Risk assessments, which may include threat/risk assessments, privacy impact assessments or other assessments as necessary, will 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.

11.2 All Risk Assessments will be undertaken by a team, led by the person accountable for the task being complete. This team will consist of the team lead and others using the RACI model, where at the least R, A and C are represented:

11.2.1 Responsible – the person or group who is responsible for performing a task

11.2.2 Accountable – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)

11.2.3 Consulted – the person or group communicated with prior to a task being performed

11.2.4 Informed – the parties who are notified about an activity before, during or after it is performed.

11.3 Risk Assessments can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

11.4 The Division Risk Assessment Questions document or the Web Tools Risk Assessment Framework should be used to evaluate risk and make recommendations to the FOIP Coordinator for any new business process, system, application or service, if it involves the collection, use or disclosure of personal or otherwise sensitive personal information.

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

11.6 Privacy impact assessments as part of the risk assessment process will be reviewed by the FOIP Coordinator, or by someone designated by that person.

11.7 Threat/risk assessments of Web Tools will be reviewed by the Technology Integration Facilitators.

11.8 Employees 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.

12. Workstation Security

12.1 Workstations include: laptops, desktops, netbooks, tablets and other computer based equipment containing or accessing Division information, including home workstations and staff owned devices accessing the Division network.

12.2 Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitivity information, including personal information as defined in the Freedom of Information and Protection of Privacy Act,

health information as defined in the Health Information Act and student information as defined in the Student Records Regulation, as well as any other information of a sensitive or confidential nature.

12.3 Employees using workstations will consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access.

12.4 The Division will implement physical and technical safeguards for all Division workstations that access electronic protected information to restrict access to authorized users.

12.5 Appropriate measures that are in place include:

12.5.1 Technical personnel and users, which include employees, consultants, vendors, contractors, and students, will be made aware and confirm awareness that compliance with the all applicable policies, procedures, and standards related to mobile and personal computing devices is mandatory.

12.5.2 Storing all sensitive information, including all personal information, on network servers, not local drives, whenever possible.

12.5.3 Securing workstations (screen lock or log out) prior to leaving area to prevent unauthorized access.

12.5.4 Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.

12.5.5 Ensuring workstations are used for authorized business purposes only.

12.5.6 Unauthorized software on workstations is not supported and will be removed on reimaging.

12.5.7 Anti-virus programs are running and up to date on devices that access the private network.

12.5.8 Monitors are positioned away from public view.

12.5.9 Wireless network access is secured.

13. Passwords

13.1 All system-level passwords (e.g. server admin, application administration accounts, etc.) must be changed regularly.

13.2 Passwords must not be inserted into email messages or other forms of electronic communication.

13.3 Secure and different passwords (each password must have a minimum of 14 characters long and must contain characters from three of the following categories: Uppercase letter, lowercase letter, base 10 digits and a non-alphanumeric character) for both your network account and your e-mail account are required. Other required passwords for Division system passwords must follow the same standard.

13.4 Passwords must never be written down and stored in an unsecured area or stored on-line unencrypted.

13.5 Passwords must never be shared.

14. Application Service Providers (ASPs)

14.1 Any business process, system or application that is proposed to be outsourced to an ASP where Division data or applications are to be hosted or affected by the ASP (that is hosted by the Division, but maintained in some way by the ASP), a binding contract with the ASP must fully specify the privacy and security measures to be employed by the ASP.

14.2 Division departments using an ASP but where data is stored on a Division server must develop logging procedures for when employees of the ASP are entering a Division system.

14.3 All ASP's must agree in writing to the following:

14.3.1 The ASP is responsible for maintaining the security and confidentiality of all personal information found in or taken from the records.

14.3.2 If hosting Division data, the ASP is responsible for identifying the persons who will have access to this personal information in a form that identifies, or could be used to identify, the individual(s) to whom it relates:

14.3.2.1 Before any personal information is disclosed to those persons listed above, the ASP will obtain a written agreement from each of them to ensure they will not disclose that personal information to any other person and will be bound by all terms and conditions of the present agreement.

14.3.2.2 The ASP will keep a copy of each such agreement and will provide the Division with a photocopy of each agreement if requested.

14.3.3 Physical security at the ASP will be maintained by ensuring that the premises are securely locked, except when one or more of the individuals named above are present, as well as by the following additional measures (e.g. locked filing cabinet):

14.3.3.1 A system of authorization and access procedures: system passwords, encryptions, and password protection.

14.3.3.2 Periodic review of access logs.

14.3.3.3 Physical security: locked doors, cabinets, etc.

14.3.4 Personal information contained in the records will not be used or disclosed for any purpose other than the project described in the proposal/contract (including additional linkages between sources of personal information), nor for any subsequent purpose, without the express written permission of the Division.

14.3.5 No personal information that identifies or could be used to identify the individual(s) to whom it relates will be transmitted by means of any telecommunications device, including telephone, fax, cable, and wireless communication networks.

14.3.6 Unless expressly authorized in writing by the Division, no direct or indirect contact will be made with the individuals to whom the personal information relates.

14.3.7 The ASP is responsible for ensuring complete compliance with these terms and conditions. In the event that the ASP becomes aware of a breach of any of the conditions of this agreement, the ASP will immediately notify the Division in writing.

14.3.8 The ASP understands that the Freedom of Information and Protection of Privacy Act specifies that a person who under the Act willfully contravenes the Act's requirements for collection, use and disclosure of personal information is guilty of an offence and liable to a fine of up to $10,000. In addition to liability for an offence, The ASP understands that the Division may take legal action against it if there is contravention of the terms and conditions of this agreement.

14.3.9 Written consent of Division must be obtained prior to the transfer of any agreement to another person, or a change in the use of the information is implemented. Consent may be arbitrarily withheld at the sole discretion of the Division.

15. Admirable Use – (Refer to AP 140 – Digital Citizenship)

Reference: Sections 31, 33, 52, 53, 56, 196, 197, 204, 222, 225 Education Act
Freedom of Information and Protection of Privacy Act
AP 140 – Digital Citizenship
AP 141 – Portable Technology Security
AP 180 – FOIP
AP 185 – Records and Information Management
AP 320 – Student Records