INFORMATION SECURITY

Background

The Division supports the use of digital environments for the purpose of supporting and enhancing teaching, learning, and business processes, including information and records management. As a result, protected information can be collected, created, and stored in electronic form. All staff have a statutory and ethical responsibility when using technology and cloud-based services to ensure appropriate care of this protected information. Staff must adhere to the provisions in Alberta's Freedom of Information and Protection of Privacy Act, the Education Act, Board policy, and Division administrative procedures.

Definitions

For the purposes of this Administrative Procedure:

Cloud-based services are applications or services externally available while outside of the Division's facilities. These may include contracted services hosted by third parties or those made available by Technology Services.

Digital Citizenship is defined as the generally-accepted behavior of responsible citizenship carried over to online environments. It can be said to include, but not limited to, the following:

- Treating others with dignity and respect;
- Respecting the privacy of others;
- Respect others by refraining from sharing information about them without their knowledge or consent;
- Respect others by refraining from using profane or abusive language;
- Respect others by refraining from posting or storing any content that contains sexual, racial, religious, or ethnic slurs, any other form of abuse, or that contain threatening or otherwise offensive language or pictures;
- Protecting your own personal information from unknown or non-understood online environments, agencies, or individuals;
- Only engaging in online financial transactions with known agencies, and only then via secure means;
- Respect others by refraining from actions that are malicious or harmful to them;
- Respecting copyright;
- Respecting and abiding by Canadian law, whether Federal, Provincial, Municipal or other statutes;

- Respecting the laws or rules of any other state, international agency or organization with whom you interact;
- Ensuring you are authorized to access resources either inside or outside of the Divisions network prior to accessing them;
- Refraining from sending files or messages designed to disrupt other computer systems or networks.

Portable storage device is deemed to be any mobile device that can store or process or transmit information digitally. This includes, but is not limited to, laptops, tablets, smartphones, thumb/portable drives, CD/DVD.

Protected information refers to all information assets collected or stored that, if compromised, could cause harm to an individual or the Division. It includes but is not limited to Personal Information defined below.

Personal Information under the FOIP Act, means recorded information about an identifiable individual, including:

- Name, home or business address, or home or business telephone number;
- Race, national or ethnic origin, colour or religious or political beliefs or associations;
- Age, sex, marital status or family status;
- An identifying number, symbol or other particular assigned to the individual;
- Fingerprints, other biometric Information, blood type, genetic Information or inheritable characteristics, and photo likeness;
- Information about the individual's health and health care history, including information about a learning, physical or mental disability;
- Information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- Another's opinion about the individual; and
- The individual's personal views or opinions, except if they are about someone else.

Privileged Access is special access or abilities above and beyond that of a standard user.

Information Stewards are the person(s), or their delegates who are responsible for determining how protected information may be used and disclosed. In most cases, this will be the Secretary-Treasurer but may include the Director of Technology Services or others in supervisory roles.

Procedures

1. The Teaching Quality Standard 3(a) states instructional strategies will include "appropriate use(s) of digital technology, according to the context, content, desired outcomes, and the learning needs of students." As such, all students using technology for learning will receive appropriate guidance from their teacher in regard to Digital Citizenship.

2. Protected Information

    2.1 All protected information shall be stored and guarded against unauthorized access.

    2.2 Access to protected information shall only be granted to those who require it as part of their duties.

3. Privileged Access

    3.1 Privileged access to protected information shall only be granted if the user is entitled to such access by virtue of their job; or in other exceptional cases where the information steward decides that the user requires temporary access to fulfill their duties.

    3.2 While fulfilling their support duties, it may be necessary for Technology Services staff or others with privileged accounts to access a user's files.

        3.2.1 For employee files, this is only permitted when authorized by the user, the Director of Technology Services or designate.

        3.2.2 For student files, this is only permitted when authorized by the Principal, Superintendent, or designate.

        3.2.3 Access will be logged in the Technology Services helpdesk or through an email to the users direct supervisor.

    3.3 An audit of privileged access can be initiated at any time by the information steward to ensure appropriate use.

    3.4 The Director of Technology Services will complete an annual privileged access audit for submission to the Secretary-Treasurer due at the end of the school year.

        3.4.1 The audit will be completed on all staff granted privileged access by the Director of Technology Services and others identified in consultation with the Secretary-Treasurer.

        3.4.2 Privileged access of the Director of Technology Services will be audited by a member of Technology Services identified by the Secretary-Treasurer.

        3.4.3 The report will include users, systems, and methods used during the audit.

        3.4.4 Inappropriate use of privileged access will be immediately reported to the Secretary-Treasurer.

4. Portable storage devices shall not be used by employees to store any protected information unless authorized to do so by the Superintendent or designate. The information must be encrypted, and password protected. Protected information on portable devices must be temporary and removed upon completion of the task.

5. Protected information must not be transferred or copied off Division systems without prior authorization of the Superintendent or designate.

6. Each user must have a unique account with a secret password.

7. User accounts may not be shared among multiple users without prior approval from the Director of Technology Services.

8. For cloud-based services where an agreement is entered into by the Division, an assessment will be completed by the Director of Technology Services before use is approved.

9. For cloud-based services where an agreement is entered into by the School the Cloud Application and Storage Risk Assessment (Appendix A) will be completed by the Principal in consultation with all stakeholders and submitted to the Director of Technology Services for approval.

10. Users of cloud-based services by staff must respect the principles of "Digital Citizenship". In addition, staff are expected to respect the following while online:

    10.1 For professional staff, the code of conduct specific to their profession;

    10.2 For support staff, the same principles of conduct that would be expected while offline;

    10.3 For all staff, ensure that you do not post or share any work-related information that would be considered confidential; and

    10.4 For all staff, understand that your actions both on and offline away from work can affect your employment relationship with the Division.

11. Division staff must report any breaches of information security, privacy, or abuse of cloud services, whether actual or suspected, to their supervisor.

    11.1 Supervisors shall contact the Director of Technology Services for assistance.

    11.2 All breaches must be reported to the Secretary-Treasurer.

    11.3 When a breach or act of abuse occurs, no action should be taken by the teacher or school, which could impede an investigation until directed to do so by the Superintendent or designate.

    11.4 No data or account information should be deleted until directed to do so by the Superintendent or designate.

    11.5 Parents, students, or other staff should not be informed of the breach or abuse until directed to do so by the Superintendent or designate.

12. The Director of Technology Services will ensure:

    12.1 All users change their secret passwords by October 15th each school year. Users who do not change their password will have their access revoked.

12.2 Employee access to cloud-based services will use multi-factor authentication methods.

12.3 Remote access to systems internal to Division facilities are to be used as a temporary measure and must use multi-factor authentication where available.

12.4 Backups are maintained for all Division data.

12.5 An Endpoint Detection and Response System is in place on all appropriate Division systems.

12.6 Only authorized persons shall have access to install applications on servers or computers.

12.7 Online training is provided annually in regard to this procedure and other information security matters to all employees annually. Staff who do not complete the training by October 15th each school year will have their access revoked.

Adopted/Revised: JUN 2016/JUN 2019/NOV 2019/SEP 2022

Reference: Section 11, 31, 33, 52, 53, 196, 197, 222 Education Act
Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
I.T.I.L. Standards, Alberta Education
ATA Code of Professional Conduct
Alberta Education Teaching Quality Standard