cbe.ab.ca

Responsible Care and Security of Information

administrative regulation

Administrative Regulation No. 1061

Classification: General

Effective Date: August 31, 2020

1 | Purpose

The purpose of this administrative regulation is to:

- provide guidelines and support for the use, responsibility, accountability and protection of CBE's information.

2 | Scope

This administrative regulation applies to:

- all Calgary Board of Education staff and all information, recorded in any form, which is owned or under the custody of the Calgary Board of Education, including all personal or organizational information.

3 | Compliance

All employees are responsible for knowing, understanding and complying with this administrative regulation.

Failure to comply with this administrative regulation may result in disciplinary action up to and including termination of employment.

4 | Principles

The following principles apply.

- CBE values the safety and security of students and staff.
- CBE values the safety and security of information collected, owned or in our custody.
- CBE staff should have access to the information necessary to carry out their duties.

5 | Definitions

CBE: means The Calgary Board of Education.

Confidentiality: means the duty of anyone entrusted with data or information to keep that data or information private and only use that information for the purpose in which it was intended.

Confidential information: means data or information that is accessible only to those authorized to have access to it. Levels of confidential information in CBE include:

- Internal data or information - this data or information is intended only for uses within CBE and is not meant for public consumption such as information, including personally identifying information,

posted to Insite, presented at meetings, obtained via email, or contained in CBE platforms such as PeopleSoft, Smart Find Express, and PowerSchool. Injury to CBE or an individual could result if data or information is inadvertently or intentionally disclosed or compromised.

- Sensitive data or information – this data or information, including information about CBE operations such as budget information, staffing reductions, policy changes and personally identifying information, is specific to a specific function, group or role. Serious injury to CBE's interests or reputation or an individual's privacy, to which they are entitled, reputation could result if data and information, is overly shared, inadvertently or intentionally disclosed or compromised.

- Highly sensitive data or information – this data or information, including information about CBE operations such as budget information, staffing reductions, policy changes and personally identifying information, will only be used for the purpose for which it was intended. Sharing will only occur with a named or specific position as needed for effective business operations. Extremely grave injury to the CBE, CBE's interests or reputation, or an individual, including the privacy to which an individual is entitled could occur if data and information is compromised.

Data and/or Information: means a collection of related data or knowledge about a topic. This may include personal, internal, operational, financial, confidential or sensitive information.

Disposition: means the disposal or transfer of data and information.

Electronic Device: means any device or media that stores electronic data and information. These include mobile devices regardless of being personally or CBE owned.

Personal information: means data and information about an identifiable individual, including name, photo, home address and phone number, age, student or employee ID number.

Personal device: means any electronic device that is not owned by the CBE and is the personal property of an individual.

Privacy: means the right to exercise control over your own personal information with the *Freedom of Information and Protection of Privacy Act* governing how public bodies must handle personal information.

Record: means information that is written, photographed, recorded or stored in any manner.

Secure connection: means a method of access that includes technical characteristics that can assist with securing communications, data and information exchanges from unauthorized parties. Secure connections typically involve strong authentication and encryption at a minimum.

Third party: means any person, group of persons or organization other than the CBE for example, file sharing providers (iCloud, Dropbox, contracted services).

Transitory record: means records that have only immediate or very short-term value and will not be required again. Examples of transitory records are advertising material, exact duplicates, external publications (i.e. magazines), routine notices such as for special events.

6 | Regulation Statement

Employee Responsibility

1) Consistent with Administrative Regulation 4027 | Employee Code of Conduct, it is the responsibility of each employee to be informed and fully understand their role regarding the proper handling and protection of data and information in their custody and control.

Supervisory Role

2) Supervisors are responsible for the establishment and communication of expectations and procedures, which conform to this regulation and provide for the security of data and information within their environment/service unit.

Information Security

3) All data and information, including internal, sensitive and highly sensitive, that is received, created, managed and maintained by CBE is the property of the CBE and subject to this regulation.

4) Only authorized persons may have access to data and information.

5) All authorized CBE staff who create, use, manage, distribute, dispose of or preserve records, data and information have a responsibility to protect those records, data and information to prevent unauthorized access, unauthorized modifications or loss.

6) All data and information (internal, sensitive, or highly sensitive) must be securely maintained in confidence throughout the entire time it is in CBE custody including creation, usage, disposition and/or preservation.

7) Personal data and information may only be disclosed 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, Youth and Family Enhancement Act* and the *Canada Income Tax Act*.

Access

8) Access to information, including internal, sensitive and highly sensitive, is restricted to those whose duties require such access and have received the appropriate authorization.

9) The use of CBE owned or managed devices, storage and sanctioned environments is compulsory.

10) Any staff member connecting personally owned devices to the CBE network must have encryption enabled and a pass code.

7 | Procedures

Security Measures

11) All employees who use personal or confidential information (internal, sensitive, or highly sensitive) in the execution of their duties shall:

a) use secure remote connections to access personal/confidential information;

b) refrain from storing anyone's personal or confidential information (internal, sensitive or highly sensitive) on non-CBE owned devices or on third party environments not sanctioned by CBE for such uses such as iCloud, Dropbox or the Google suite of applications;

c) refrain from using third party tools or environments not sanctioned by CBE, such as Zoom and WebEx, for online conferencing or collaboration, including audio, video, screen sharing, and instant messaging, when the conference/collaboration involves confidential (internal, sensitive or highly sensitive) or anyone's personal information;

d) ensure that all information (internal, sensitive or highly sensitive) stored on mobile or personal devices is encrypted and password protected;

e) copy, download, print or transport only the information (internal, sensitive or highly sensitive) that is required for specific tasks;

f) keep paper records and mobile or personal devices physically secure;

g) maintain an inventory or copy of the information (internal, sensitive or highly sensitive) temporarily stored at home or on mobile or personal devices under their control;

h) ensure that the master copy of information (internal, sensitive or highly sensitive) is stored on a centralized CBE system;

i) destroy or remove transitory paper, digital or electronic records information (internal, sensitive or highly sensitive) according to CBE Corporate Records Management when it is no longer required to carry out their duties;

j) not leave mobile or other portable storage devices unattended or in non-secured areas; and

k) ensure reasonable precautions are taken which are consistent with the level of confidentiality as defined in the Confidentiality Protocol of the data under their custody.

Storage of Data and Information

12) Data or information (internal, sensitive or highly sensitive) must be stored in a secure manner with access restricted to those authorized.

Use and Disclosure of Data and Information

13) Use of data and information (internal, sensitive or highly sensitive) is limited to the specific purpose for which it was collected.

14) All information (internal, sensitive or highly sensitive) that is collected will be for a stated purpose which is clearly communicated upon collection.

Disposal of Data and Information

15) The disposal of information must be in accordance with CBE's Classification and Retention Schedule as outlined by CBE Corporate Records Management.

16) Paper documents must be disposed of by secure shredding.

17) Digital documents must be disposed by permanent deletion.

Retention of Data and Information

18) The retention of information must be in accordance with the CBE's Classification and Retention Schedule as outlined by CBE Corporate Records Management.

19) Only the information (internal, sensitive or highly sensitive) that is required must be retained.

Transportation of Data and Information

20) It is the responsibility of the sender to ensure that personal, internal, sensitive, and highly confidential information, when being shared, transported or transferred, reaches the intended recipient intact without unauthorized access, change or disclosure (for example; correct user and/or username, fax number or email address, data encryption, sealed envelopes, keeping it on your person, not leaving the information or device unattended etc.).

Use of Third Party

21) Individual or groups must not use unsanctioned third party providers for distribution or storage of personal or confidential internal, sensitive, and highly sensitive information, i.e. iCloud, Dropbox, etc., unless Information Technology Services approval has been received.

Distribution of Data and Information

22) Information shall only be shared or distributed to those whose duties require such information and have the appropriate level of authorization to access. This includes data and information shared in meetings, dialogue sessions, or other collaborative sessions.

23) It is the responsibility of the sharer to ensure that all recipients are made aware of the confidentiality (internal, sensitive, highly sensitive) of the information being shared and they understand that they are not authorized to distribute or share the information without prior approval.

24) Any email correspondence will include a privacy message stating the intended recipient and actions to be taken if received in error.

25) Personal or confidential operational or business information that is internal, sensitive, or highly sensitive information should not be disclosed, in any form, to unauthorized persons.

Reporting Loss of Data and Information

26) If CBE information is lost, stolen, inadvertently or intentionally disclosed or compromised, the employee must inform their supervisor immediately upon discovery, and make the following contacts:

a) for CBE owned devices, contact the help desk; and

b) for personal devices that contain CBE information, contact the FOIP Coordinator.

8 | History

Approval	August 31, 2020
Next Review	August, 2025
Revision/Review Dates	August 2001 February 2003 May 2013

9 | Related Information

- *Education Act*, S.A. 2012 c. E-0.3
- *Alberta Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c F-25
- *Alberta Child, Youth and Family Enhancement Act*, R.S.A. 2000, c C-12
- *Canada Income Tax Act*
- *Children First Act*

- AR 1062 | Responsible Use of Electronic Information Resources
- AR 4027 | Employee Code of Conduct
- AR 6024 | Student Records

- CBE Visual Identity Standards (email confidentiality statement) https://insite.cbe.ab.ca/Forms%20%20Manuals/Visual-Identity-Standards.pdf#page=21
- Records Classification and Retention Schedule https://insite.cbe.ab.ca/Forms%20%20Manuals/Corporate-Records-Classification-and-Retention-Schedule.pdf
- Resources for FOIP and confidentiality
- https://insite.cbe.ab.ca/organization/inside_cbe/legal_services/Pages/default.aspx