Clearview Public Schools
We All Belong – We All Succeed

Administrative Procedure 142 - Information Security

Background

Other than data defined as public, all data and processing resources on the Division network are only accessible on a need-to-know basis to specifically identified, authenticated and authorized users.

Network Security involves the protection of all data, applications, networks, and computer systems from all threats, whether it be unauthorized or inappropriate access, usage, alteration, disclosure or destruction either internally or externally, deliberate or accidental.

Procedure

1. The Director of Technology Services will ensure that:
    1.1. information is protected against unauthorized access;
    1.2. confidentiality of information is assured;
    1.3. integrity of information is maintained;
    1.4. information security training is provided;
    1.5. a disaster recovery plan is produced, maintained and tested annually;
    1.6. availability of information and information systems for business and educational needs is met;
    1.7. Legislative, regulatory and Division procedure requirements are met;
    1.8. associated administrative procedures are produced and updated as needed.

2. Site Administrators/Principals/Supervisors are responsible for ensuring implementation of the administrative procedures within their areas of responsibility and for the adherence of staff and students.

3. It is the responsibility of each user accessing any aspect of the Division's information system to do everything reasonable, within their power, to ensure any/all procedures, standards or guidelines are followed.

4. Division staff must report any breaches of information security, whether actual or suspected, to their immediate supervisor for investigation. Supervisors shall contact the Director of Technology for assistance.

5. This Administrative Procedure applies to all Division data assets that exist in any Division applications, systems, or network environments on any media during any part of its life cycle. The Administrative Procedure applies to all systems and data, whether academic,

administrative or any other. The following users are covered by this Administrative Procedure: Full or part-time employees of the Division, contractors, volunteers and visitors, any other persons, entities, or organizations that have access to Division data, applications, systems, or network environments.

6. The Director of Technology Services shall be responsible for establishing, maintaining, implementing, administering, and interpreting organization-wide information systems security standards, guidelines, and procedures. While responsibility for security of information systems on a day-to-day basis is every employee's duty, specific guidance, direction, and authority for information systems security is centralized for all of the Division through the Director of Technology.

7. The Director of Technology Services is further responsible for:

    7.1. securing data for investigations into any alleged computer or network security compromises, incidents, or problems. Such requests must be submitted in writing by the Superintendent;

    7.2. providing security guidance to school administrators, department directors, coordinators/ supervisors and senior leadership;

    7.3. promoting security awareness to all users of the Division information system.

8. The Director of Technology Services shall, in conjunction with senior leadership, review this document on an annual basis.

9. A contingent review shall be conducted if a significant loss occurs due to a risk that has not been adequately addressed by administrative procedures.

Reference: Section 31, 32, 33, 52, 53, 196, 222 Education Act
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

Effective: 2010-06-23
Amended: 2020-08-30, 2024-01-23