REGULATION #5700.2
COLLECTION, PROTECTION AND ACCESS TO PERSONAL INFORMATION

1. DEFINITIONS

1.1. Personal Information as defined in the Act includes:

a) The individual's name, address and telephone number.

b) The individual's race, national or ethic origin, colour, religious or political beliefs or associations.

c) The individual's age, sex, sexual orientation, martial status or family status.

d) An identifying number, symbol or other particular assigned to the individual.

e) The individual's finger prints, blood type or inheritable characteristics.

f) Information about the individual's health care history, including a physical or mental disability.

g) Information about the individual's educational, financial, criminal or employment history.

h) Anyone else's opinions about the individual.

i) The individual's personal view or opinions, unless they are about someone else.

2. COLLECTION & PROTECTION OF PRIVACY

2.1. Personal information may only be obtained as authorized in the Act and used for the specific purposes for which it is gathered. Confidentiality must be protected by each employee who is authorized to have access to personal information. The management and safekeeping of such information is the responsibility of each designated employee.

2.2. Employees of the board have the duty to make every reasonable effort to ensure the accuracy of personal information. An individual who believes that his or her personal information contains an error or omission may request correction of that information.

2.3. Each department is responsible for the security of personal information, its accuracy and documentation. Each file shall be maintained in a comprehensible manner and will contain a record of those employees who have had access to it, who would not normally have access in the normal course of their duties.

REGULATION #5700.2
COLLECTION, PROTECTION AND ACCESS TO PERSONAL INFORMATION

3. REPORTING PRIVACY BREACHES

3.1. Employees must ensure a breach (compromise) or suspected breach of security involving personal information is reported to the district's privacy officer as soon as possible after the breach or potential breach is discovered.

4. PERSONAL INFORMATION BANKS

4.1. A listing or directory of all personal information must be maintained by each department indicating who is responsible for it, what form it takes and who has access to it. A master list of Personal Information Banks will be maintained by Communication Services Department.

5. RETENTION

5.1. Any personal information of a private individual that is no longer required for either administrative, financial, legal or historical purpose and its retention is not regulated by any statute, may be destroyed in a confidential manner (i.e. shredding) as outlined in retention schedule.

6. ACCESS TO PERSONAL INFORMATION

6.1. Approval for the release of personal information under the Act is the responsibility of the superintendent of schools.

6.2. Use of personal information must be consistent with the purposes for which the information was obtained or compiled.

6.3. Access to personal information is available to:

a) Authorized board employees who require access for the conduct of their duties as specified in the Act.

b) The individual or legal guardian.

c) Other parties (e.g. legal counsel of the employee or board) with authorized written consent of the individual.

6.4. Applications for access to personal information must be made in writing by the individual. Every official application made under the Act will be passed to the Manager, Communication Services. The request will then be directed to the appropriate department head for retrieval.

6.5. All responses to an application for access to personal information, whether granted or denied will be directed to the Manager, Communication Services for review and final documentation and then forwarded to the individual making the request within thirty days after receipt of the application.

6.6. Once approved, access can be gained in person during normal business hours, upon appointment. Applicants must be given access only in the presence of a supervisory officer, personnel officer or other board official. A record of all such transactions must be kept in the file where the information resides.

7. TIMELINES

7.1. In the event that a response to an application for access cannot be completed within the thirty-day time limit due to circumstances specified in the Act, the individual making the request will receive written notice of the extension setting out:

a) The length of the extension

b) The reasons for the delay

c) The person's right of appeal to the Freedom and Privacy Commissioner to review the extension

8. ERROR OR OMISSIONS

8.1. An applicant who believes there is an error or omission in his or her personal information may request in writing to the designated authority to correct the information. The department head or designate is responsible for the correction for annotation of the information.

8.2. Notification of the correction must be given to any other public body or third party to whom that information has been disclosed during the one-year period before the correction was requested.

8.3. Any correction, annotation or notification must be documented by the department head or designate.

Revised: 2016-06-03
Approved: 1995-06-22