The Board of Education of
School District No. 83 (North Okanagan-Shuswap)

BRIEFING NOTE

TO:	Board of Education	**DATE:**	19 January 2021
FROM:	Peter Jory, Superintendent of Schools/CEO		
RE:	**Policy 250 – Freedom of Information and Protection of Privacy**		

Background

Policy 250 – Freedom of Information and Protection of Privacy (formerly Policy 3070) has been revised as part of the Policy Manual renovation. First reading was approved by the Board on September 17, 2019.

Revisions to the policy are minor wordsmithing edits and formatting only. It is being presented to the Board for second and final reading at this time.

Recommendation

That the Board of Education approve the second and final reading of Policy 250 – Freedom of Information and Protection of Privacy (formerly Policy 3070) as presented.

Respectfully submitted,

Peter Jory
Superintendent of Schools/CEO

POLICY 250 FREEDOM OF INFORMATION and PROTECTION OF PRIVACY

The Board of Education of School District No. 83 (North Okanagan-Shuswap) is a public body subject to the provincial BC Freedom of Information and Protection of Privacy Act (FIPPA) and the *School Act*. Both statutes contain provisions that regulate the public's access to information held by the District and govern the District's responsibilities to protect personal information from unauthorized access, use or disclosure. Also, the District must ensure that all personal information held in its custody and control is protected by reasonable security arrangements. Relevant guidelines in FIPPA will be followed when making decisions to retain or dispose of information. *'Under FIPPA, a public body must retain personal information for at least one year after it is used to make any decision'* (FIPPA, *School Act,* Collective agreements, HR Guidelines, other district policies).

Guidelines

1. **Personal Information**

Under the FIPPA, "personal information" means any information about an identifiable individual. Personal information may include data such as unique identifiers (Personal Education Number (PEN) or SIN), school records, **personal** contact numbers, gender, medical history, education, employment, psychiatric history, behavioural assessments, personnel evaluations, digital images, audio and video recordings, racial or ethnic origin, sexual orientation or religious beliefs.

2. **Employee Personal Information**

Employee personal information is any recorded information about an identifiable employee (see Personal Information above) other than contact information. The release and sharing of contact information **for an employment purpose** is not a privacy violation.

3. **Student Personal Information**

Student personal information includes Personal Information (defined above) plus any information that identifies a student including the student's name, address, and contact numbers, PEN, assessments, results, and educational records. District employees may disclose student personal information to other District employees where such disclosure is necessary for the performance of the duties of the employee and to other school districts where it is necessary for educational purposes.

4. Collection of Personal Information

The District has the legal authority to collect personal information that relates directly to and is necessary for its operating programs or activities or as otherwise authorized by statute. Personal information will be collected directly from the individual unless another method of collection is authorized by the individual or the statute.

When a school or the District collects personal information about students or families, parents/guardians should be informed of the purpose for which the information is being collected. The parents/guardians of a student must authorize the disclosure of personal information for purposes ancillary to educational programs such as:

- newsletter publications;
- website postings;
- video conferencing;
- social media applications;
- honour roll lists;
- team rosters; or
- Yearbooks.

Parents/guardians will complete and submit the form titled Student Registration Form – Freedom of Information and Protection of Privacy upon their child's initial enrollment. Where the parent or guardian provides consent, this will allow the school or the District to publish student personal information, **including photographs,** for purposes such as:

- recognition of achievement;
- promotion of events; or
- commemoration of school events.

The authorization is deemed in effect until the student changes or transitions to another school. Parents/guardians will have the ability to opt out of providing information that is not directly related to a student's educational program or necessary for the District's operational activities. Posting of personal information such as exam results should not contain student identifiers.

5. Use of Personal Information

Personal information will be used for the purpose for which it was collected or for a use consistent with that purpose. Should there be a need to access information for a purpose other than why it was collected or if there is uncertainty as to the confidentiality of the information; clarification will be provided from the District Privacy Officer (Secretary-Treasurer) in keeping with the FIPPA.

6. Disclosure of Personal Information

Personal information may be disclosed to an external or third party if the individual who is the subject of the information has provided written consent. In the case of a student under age nineteen, such consent may be provided by the student's parent or guardian.

Disclosure of personal information should not occur in any situation or in any physical location that may compromise confidentiality.

District employees have a right to access District records in its control and custody, providing it's required to complete the duties of their work assignment.

A custodial parent or guardian has the right to access personal information on behalf of their child under the age of nineteen.

The District governs the right of access by an individual to his/her own personal information and by the public to any information or records in its custody or control of the District.

School districts, other government ministries, or law enforcement agencies may have access to personal information where obtaining this information is necessary for the provision of their services.

7. Securing Personal Information

Information management must be dealt with in a responsible, efficient, ethical, and legal manner. Users of electronic network resources should not disseminate personal information to anyone not covered by a confidentiality agreement, also precautions should be taken to ensure information is protected from unauthorized access, use, and disclosure. All District employees are expected to maintain, secure, and retain appropriate student and personnel records in a manner that respects the privacy of employees, students and students' families and complies with the regulations specified in FIPPA and the *School Act.*

The following safeguards, though not an exhaustive list, will assist in protecting privacy of personal information for both students and employees:

- security (e.g. passwords, encryption) must be in place for personal information, stored, printed, or transferred by computers;
- all electronic mobile devices (even personally owned devices) that access or store District data must be secured by a password log-on and use the highest available encryption options;
- electronic mobile devices that contain or can access District data should be kept on one's person **or never be left unsecured** in public areas (i.e. classrooms, hotel rooms);
- passwords should not be shared nor should anyone logon to a system using an ID that has not been specifically assigned to them; and
- paper files should be safeguarded by implementing reasonable security precautions:

    - locked storage;
    - removal of personal information from work areas; and
    - shredding of documents containing personal information.

Access to any personal information should be based on employment duties requiring such access. Unauthorized access to information about colleagues, friends, or family is not permitted. Any personal information that is no longer required for administrative, financial, or legal purposes will be destroyed in a confidential manner when no longer needed for these purposes. Paper files due for destruction should be securely shredded and destroyed. Computer files should be deleted in their entirety and any data storage devices should be fully erased prior to disposal (i.e. computers, Multi Functional Devices, printers).

8. Reporting of Complaints

Anyone suspecting or aware of the unauthorized collection, use, access, or disclosure of student or employee personal information, breach of confidentiality protocols or contraventions of this Policy must report such activities to the District Privacy Officer (Secretary-Treasurer) who will determine appropriate action if necessary and report back to the complainant.

POLICY 250 FREEDOM OF INFORMATION and PROTECTION OF PRIVACY

The Board of Education of School District No. 83 (North Okanagan-Shuswap) is a public body subject to the provincial BC Freedom of Information and Protection of Privacy Act (FIPPA) and the *School Act*. Both statutes contain provisions that regulate the public's access to information held by the District and govern the District's responsibilities to protect personal information from unauthorized access, use or disclosure. Also, the District must ensure that all personal information held in its custody and control is protected by reasonable security arrangements. Relevant guidelines in FIPPA will be followed when making decisions to retain or dispose of information. *'Under FIPPA, a public body must retain personal information for at least one year after it is used to make any decision'* (FIPPA, *School Act,* Collective agreements, HR Guidelines, other district policies).

Guidelines

1. **Personal Information**

Under the FIPPA, "personal information" means any information about an identifiable individual. Personal information may include data such as unique identifiers (Personal Education Number (PEN) or SIN), school records, **personal** contact numbers, gender, medical history, education, employment, psychiatric history, behavioural assessments, personnel evaluations, digital images, audio and video recordings, racial or ethnic origin, sexual orientation or religious beliefs.

2. **Employee Personal Information**

Employee personal information is any recorded information about an identifiable employee (see Personal Information above) other than contact information. The release and sharing of contact information **for an employment purpose** is not a privacy violation.

3. **Student Personal Information**

Student personal information includes Personal Information (defined above) plus any information that identifies a student including the student's name, address, and contact numbers, PEN, assessments, results, and educational records. District employees may disclose student personal information to other District employees where such disclosure is necessary for the performance of the duties of the employee and to other school districts where it is necessary for educational purposes.

4. Collection of Personal Information

The District has the legal authority to collect personal information that relates directly to and is necessary for its operating programs or activities or as otherwise authorized by statute. Personal information will be collected directly from the individual ~~the information is about~~ unless another method of collection is authorized by the individual or the statute.

When a school or the District collects personal information about students or families, parents/guardians should be informed of the purpose for which the information is being collected. The parents/guardians of a student must authorize the disclosure of personal information for purposes ancillary to educational programs such as:

- newsletter publications;
- website postings;
- video conferencing;
- social media applications;
- honour roll lists;
- team rosters; or
- ~~yearbooks~~Yearbooks.

Parents/guardians will complete and submit the form ~~en~~titled Student Registration Form – Freedom of Information and Protection of Privacy upon their child's initial enrollment. Where the parent or guardian provides consent, this will allow the school or the District to publish student personal information, **including photographs,** for purposes such as:

- recognition of achievement;
- promotion of events; or
- commemoration of school events.

The authorization is deemed in effect until the student changes or transitions to another school. Parents/guardians will have the ability to opt out of providing information that is not directly related to a student's educational program or necessary for the District's operational activities. Posting of personal information such as exam results should not contain student identifiers.

5. Use of Personal Information

Personal information will be used for the purpose for which it was collected or for a use consistent with that purpose. Should there be a need to access information for a purpose other than why it was collected or if there is uncertainty as to the confidentiality of the information; clarification will be provided from the District Privacy Officer (Secretary-Treasurer) in keeping with the FIPPA.

6. Disclosure of Personal Information

Personal information may be disclosed to an external or third party if the individual who is the subject of the information has provided written consent. In the case of a student under age nineteen, such consent may be provided by the student's parent or guardian.

Disclosure of personal information should not occur ~~when using a mobile phone~~in any situation or in any physical location that may compromise confidentiality.

~~Employees of the~~ District employees have a ~~general~~ right ~~of~~ to access ~~to any~~District records in ~~the~~ its control and custody~~ or under the control of the District~~, ~~provided that access is~~ providing it’s required to complete the duties of their work assignment.

A custodial parent or guardian has the right to access personal information on behalf of their ~~a~~ child under the age of nineteen.

The District governs the right of access by an individual to his/her own personal information and by the public to any information or records in its custody or control of the District.

School districts, other government ministries, or law enforcement agencies may have access to personal information where obtaining this information is necessary for the provision of their services.

7. Securing Personal Information

Information management must be dealt with in a responsible, efficient, ethical, and legal manner. Users of electronic network resources should not disseminate personal information to anyone not covered by a confidentiality agreement, also precautions should be taken to ensure information is protected from unauthorized access, use, and disclosure. All District employees are expected to maintain, secure, and retain appropriate student and personnel records in a manner that respects the privacy of employees, students and students' families and complies with the regulations specified in FIPPA and the *School Act.*

The following safeguards, though not an exhaustive list, will assist in protecting privacy of personal information for both students and employees:

- security (e.g. passwords, encryption) must be in place for personal information, stored, printed, or transferred by computers;
- all electronic mobile devices (even personally owned devices) that access or store District data must be secured by a password log-on and use the highest available encryption options;
- electronic mobile devices that contain or can access District data should be kept on one's person **or never be left unsecured** in public areas (i.e. classrooms, hotel rooms);
- passwords should not be shared nor should anyone logon to a system using an ID that has not been specifically assigned to them; and
- paper files should be safeguarded by implementing reasonable security precautions:
    - locked storage;
    - removal of personal information from work areas; and
    - shredding of documents containing personal information.

Access to any personal information should be based on employment duties requiring such access. Unauthorized access to information about colleagues, friends, or family is not permitted. Any personal information that is no longer required for administrative, financial, or legal purposes will be destroyed in a confidential manner when no longer needed for these purposes. Paper files due for destruction should be securely shredded and ~~disposed of~~destroyed~~;~~. ~~computer~~Computer files should be deleted in their entirety and ~~;~~ any data storage devices should be fully erased prior to disposal (i.e. computers, Multi Functional Devices, printers).

8. Reporting of Complaints

Anyone suspecting or aware of the unauthorized collection, use, access, or disclosure of student or employee personal information, breach of confidentiality protocols or contraventions of this Policy must report such activities to the District Privacy Officer (Secretary-Treasurer) who will determine appropriate action if necessary and report back to the complainant.