School District #62 (Sooke)

GOVERNANCE OF FOIPPA - ACCESS TO INFORMATION	No.: D-330
	Effective: Jan. 24/95 Revised: Jan. 28, 2020; June 27/23 Reviewed: Nov. 5/19; Nov. 26/19; Jan. 28, 2020; May 2/2023; May 23/23; June 27/23

ADMINISTRATIVE REGULATIONS

General Information

The Sooke School District Board of Education is committed to being transparent to the public in granting access to access to records requested by the public in conformance with the BC *Freedom of Information and Privacy Protection Act* (FOIPPA).

It is legislatively required to ensure that the public has a right to access records in the District's custody. Individuals have a right of access to, and a right to request correction of, personal information about themselves and prevent unauthorized collection, use, or disclosure of personal information by public bodies, and where possible specifying limited exceptions to the right of access.

The following schedule outlines the responsibilities of the Superintendent/CEO (Head) and the Chief Information Officer and Executive Director of Digital Solutions regarding the Freedom of Information Part 1 of the *Act*.

Responsibility	FOIPPA Section(s)
INFORMATION RIGHTS	
Decide on severing a record	4
Decide on duty to create a record	6
Decide on content of a response	8
Decide how access will be given	9
Extend time limit up to 30 days	10
Request Commissioner's approval of extension	10
Transferring a request	11
Decide to apply exceptions	12-22
NOTICE TO THIRD PARTIES	
Third Party Notice	23
Notice of Decision	24
Other Notices	22, 33, 25
PUBLIC INTEREST PARAMOUNT	
Disclosure in the Public Interest	25
REPORTS	
Annual Statistical report to Information and Privacy Branch pertaining to FOI Requests	68
Maintain School District 68's information in FOI Directory	69
Make copies of directory available	69
Make policy manuals available	70

FEES	
Assess fees, give fee estimate, require fee deposit	75
Approve waiver of fees	75

Guiding Principles

- Ensure that the School District responds to an applicant who makes a request under the Freedom of Information (FOI) sections of the legislation.
- Individuals have a right of access to a record in the custody or under the control of the School District, including a record containing personal information about the applicant.
- Be open and transparent about the information rights and how to exercise them by making every reasonable effort to assist applicants needing access to a record.
- Ensuring the confidentiality of the information contained in the staff and student records and ensuring privacy for staff, students, and their families.
- Endeavour to support our employees in understanding their data handling responsibilities.
- Collecting and using personal information only as necessary to carry out authorized programs and services.
- Support the timely response to access requests submitted under FOIPPA.
- Ensure that a process for completing and documenting FOI requests is supported and information on how to make a request is documented.
- Refusing to respond to an applicant request if a record containing information described is information harmful to law enforcement, or a record containing information would harm the financial or contractual interests of the district.
- Ensure consent is obtained for any information record related to a third party affiliated with the information record if disclosure of the existence of the information would be an unreasonable invasion of that party's personal privacy.

Exemptions

- Exception to this policy will require the Executive to make a recommendation to the Board and will adhere to the exceptions detailed in the FOIPPA.

Section I – Access to Information

Requesting a Record:

- Any member of the public may make a written request to access or correct information under FOIPPA.
- To be processed, the request must be a "complete request". To ensure that a request has been adequately filled out and contains all the necessary elements, a requester must ensure they are seeking records, not information or answers to questions that can be readily obtained on the SD62 website or from other sources. The form is available via https://www.sd62.bc.ca/freedom_of_information_request
- Under the FOI Legislation, the School district must log the business date the request was received along with other dates during the request fulfillment process and confirm receipt with the requester.
- If the request is not clear and additional information is needed within the thirty (30) day deadline, the requester may be contacted for additional information to find and narrow the search for the record or, for correction requests, to provide evidence that the information on file is incorrect or incomplete.
- The time limit for responding will be suspended written notice of the additional information needed to continue with the search or to discontinue the search is received.

Searching for a Record:

- With sufficient information to locate the record, forward the request to Foippa@sd62.bc.ca if the request for access to records is complete with sufficient detail to enable the identification of the records sought.
- Before commencing a search for responsive records, the SD62 (the District) will consider whether a time extension or fee estimate is required. If the request appears likely to require an investment of three (3) hours or more of search and/or preparation time, the SD62 will develop an estimate of the amount of time required to search for responsive records and will then prepare and provide a letter to the Requester notifying them of the fee estimate and seeking a deposit in accordance with FOIPPA legislation proposed fee charges.
- If at any time during the processing of the request, it becomes apparent to the District that it will not be possible to complete the processing of the request within the original thirty (30) day timeline for responding under FIPPA, the District will, where permitted under FOIPPA, issue a notice of extension of time in writing to the Requester, indicating the reason for the extension and the amount of additional time which is required.
- When the District receives a request, it will conduct a reasonable search, which entails the following steps:
    - FOI Coordinator will seek to clearly understand the search parameters prior to conducting the search.
    - FOI Coordinator will initiate the record search and ensure all relevant documents are retained, including transitory records that are responsive.
    - The FOI Coordinator will conduct searches and instruct staff that while collecting records in response to an access to information request, they must also search for and produce any relevant records from instant messaging and personal email accounts,
    - The FOI Coordinator will:
        - provide clear search instructions to employees participating in the search.
        - identify all databanks and places to be searched and develop a search plan.
        - document search steps.

- Upon completing the reasonable search, the FOI Coordinator shall:
    - determine whether the information requested can be retrieved in whole or in part.
    - estimate the time and cost needed to search for, retrieve and prepare the information for release.
    - forward the information requested along with a recommendation for or against disclosure to the FOI Coordinator, who, in turn, will seek discussion with the respective head of the school, department, or program area.

Review of Records and Third-Party Notification

- The District will review the records in order to determine what information therein may be exempted and/or excluded, and exercise discretion with respect to the application of exemptions as required by FOIPPA section 22 in regard to disclosing or releasing personal information about another person if the disclosure would be an unreasonable invasion of that person's privacy.
- Where the District is considering releasing records that potentially contain confidential information pertaining to a third party, the District will provide the third party with an opportunity to provide representations with respect to the disclosure of the information in question.
- Where third-party notification is required, the District will send a letter to the affected third party containing the following:
    - A statement that the SD62 intends to release a record or part of a record that may affect the interests of the person or organization.
    - The contents of the record or the part that relates to the affected person.
    - That the affected person must make representations in writing as to why the record in whole or in part should not be released; and
    - That the affected person has twenty calendar (20) days after the notice is given to reply.
- Upon receipt of the affected third party's response, the District will consider the comments sent by the affected third party and decide whether to release the information contained in the record, which may be third-party information within the time prescribed by FOIPPA.
- If the District Privacy Office decides that a record containing the affected third-party information will be disclosed to the requester, the District will inform the affected third party of this decision and of their right to appeal such decision to the Office of Information Commissioner (OIPC) within 30 business days from the date the District has notified the decision. The District will hold the records until the appeal period of 30 business days has elapsed. Once the appeal period has passed, the Privacy Officer must confirm with the OIPC that no appeal has been received before releasing the records to the requester.

How access will be given (Release of Record)

- If a fee estimate was not provided to the Requester before commencing a search for responsive records, and it appears after completing the search that greater than 3 hours of combined search and preparation time will be required to process the request, the District will provide the Requester with a fee estimate before proceeding further, which will be prepared in accordance with FOIPPA and the Regulations thereunder. The records will not be released until payment has been received in full by the District. The Privacy Officer may, however, exercise discretion to waive fees.
- If access to the records is to be provided, the information will be released to the requester within the applicable deadline set out under FOIPPA, subject to any time extensions, which may be imposed as set out above.

- If access to the records is denied the District will send a letter to the requester indicating the reasons for refusal and his/her right of appeal to the OIPC for review of the decision within 30 business days after the District has communicated the decision.

- The District will retain the responsive records, including transitory records or operational records whose retention period has expired, until the appeal period of 30 business days has elapsed, and the District has received confirmation by the OIPC that no appeal has been filed.

Appeal and File Closed

- If the requester disagrees with the District's decision, the requester may file an appeal with the OIPC pursuant to FOIPPA.

- The appeal shall be made in writing to the OIPC within thirty (30) business days from the date of the District's letter informing the requester of the decision.

- The District may participate in any mediation conducted by the OIPC and respond to the issues on appeal.

- The District shall close the access request upon its completion or final disposition by the OIPC on appeal, or if the requester:

    - Has not provided the SD62 with sufficient clarification regarding the scope of the access request within thirty (30) calendar days following the SD62's request for such clarification.

    - Has not paid in full the fees associated with the access request within thirty (30) calendar days of being informed of the fee estimate or assessment.

    - Has not filed an appeal of a decision with the OIPC within the prescribed appeal period or has exhausted all rights of appeal to the OIPC; or

    - Otherwise has not responded to correspondence from the District within thirty (30) calendar days from the date of the correspondence.

Correction Request (section 29)

- If a request for correction is requested through the FOI process, the FOI coordinator will assess the record that is deemed incorrect or incomplete by the requester.

- This shall be forwarded back to the requestor by the FOI Coordinator or to the School or Department Program Area concerned, along with the time remaining to comply with the request.

- Upon reviewing the correction request, the FOI Coordinator will:

    - determine whether the information submitted for correction contains errors or omissions; and

    - seek clarification from the school or department program lead.

- If the correction is made, the District will notify the requestor with a copy of the corrected record within the applicable deadline set out under FOIPPA.

- If the correction is denied, the District will send a letter to the requester indicating the reasons for refusal and the right of appeal to the OIPC for review of the decision within 30 business days after the District has communicated the decision. The District will advise the individual that he/she can require that:

    - a statement of disagreement be attached to the information reflecting any correction that was requested but not made; and

- any person or body to whom the personal information has been disclosed within the year before the time a correction is requested or a statement of disagreement is required, be notified of the correction or statement of disagreement.

Exceptions (Sections 12-22)

- The District will determine under FOIPPA subsection (1) or (3) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, including whether the third party will be exposed unfairly to financial or other harm, and/or unfairly damage the reputation of any person referred to in the record requested by the applicant.

Section II – Cyber Security and Privacy Breach Protocol

Introduction

The Freedom of Information and Protection of Privacy Act (FOIPPA)(Section 36.3) requires the SD62 Privacy Officer to formalize and make mandatory the escalation protocol of cyber security and privacy incidents to ensure the timely notification of any incidents, which impact SD62 community members. The Privacy Officer must notify an affected individual if a privacy breach could reasonably be expected to result in significant harm to the individual, including identity theft or other significant harms to be Section 36.3 also requires the Privacy Officer to notify the Information and Privacy Commissioner (the Commissioner) when the significant harm threshold is met. Additionally, the SD62 Cyber Risk and Security Policy and administrative regulations section 11: Information Security and Privacy Breach Incident Management, requires all breaches of information security must be investigated and reported.

Escalation Protocol for Reporting Breaches

Incident Reporting and Assessment

As per the Cyber Risk and Security Policy and Regulations, Staff must report suspected security and privacy incidents to their Supervisor immediately and notify the Chief Information Officer through the Manager, Cyber Security, and Privacy, of any suspected or actual cyber security or privacy incidents, whether major or minor. Suspected incidents can also via reported via foippa@sd62.bc.ca

The Manager, Cyber Security, and Privacy leads incident management response activities and requests internal resources (or contractors) as needed to contain and investigate the incident.

Upon being notified of a suspected incident, the Manager, Cyber Security, and Privacy will immediately and on a preliminary analysis identify the scope, nature, and probable extent of the impact of the incident and take the necessary steps to contain it.

While incident containment and possible eradication are the priorities, the Manager, Cyber Security, and Privacy will undertake a preliminary risk assessment to determine whether the incident needs to be escalated to senior management and the potential notification required.

The primary factors that are relevant to determining the extent of notification required are:

1. Risk for the District - this risk analysis is carried out using an approved Threat Escalation procedure.

2. Risk for the affected individuals - the risk analysis is carried out using an approved Threat Risk Assessment (TRA) tool.

The outcomes of the assessment completed using the tools mentioned above will assist in the internal notification process. In addition to the notifications outlined in this protocol, the Manager, Cyber Security, and Privacy through the Chief Information Officer may elect to notify other stakeholders (e.g. Executive Director, Human Resources) as required.

Cyber Security and Privacy Manager

Incidents that present a low risk for the District and the affected individuals (e.g., misdirected email that does not contain sensitive data) will usually not be escalated unless the circumstances described in the subsections below apply. Other related IT and Cyber related incidents that might have a low impact on sensitive data may not be escalated.

Privacy Officer - Chief Information Officer (CIO) And Executive Director, Digital Solutions (IT)

The Manager, Cyber Security, and Privacy will report to the CIO incidents that present a high risk for the District and the affected individuals to the extent that:

- The investigation uncovers a threat or a vulnerability (e.g., system flaw, errors in system configuration) that may be further exploited and requires coordination with IT resources and/or resources from other program areas or departments to be fixed.
- There is a pattern of similar incidents that may indicate systemic issues that need to be addressed, such as technological-related problems.
- The CIO may elect to notify the Superintendent, including the Executive and the Board of the above incidents at his discretion.

Superintendent and the Executive

The Manager, Cyber Security, and Privacy will report, through the CIO, to the Executive the following incidents:

- Incidents requiring notification to the affected individuals and/or the Information Privacy Commissioner of BC, regardless of the impact on the School District.
- Incidents presenting a moderate risk to the District (e.g., incidents affecting isolated IT environments; incidents involving limited disruption of school facilities and eventual business operations, e.g. TikTok).
- The Superintendent may elect to notify the Board of the above incidents at their discretion.

Trustees of the Board of Education

The Manager, Cyber Security, and Privacy will report, through the CIO and the Executive the following incidents:

- Incidents requiring notification to the affected individuals and/or the Office of Information Privacy Commissioner that affect many individuals or that stem from criminal activity (e.g., ransomware or theft of equipment affecting learner or employee data.;
- Incidents requiring notification to the Ministry of Education.
- Incidents that are likely to attract media attention.
- Incidents presenting a high or critical risk to the District (e.g., incidents involving disruption of School Board business operations over a sustained period; incidents affecting multiple IT environments).
- Incidents affecting individuals from other organizations or institutions (e.g., students from other school districts).
- The Board may elect to also notify the Public of the above incidents at their discretion.

Mandatory Notification to Affected Individuals

The Privacy Officer is required to provide mandatory notification to affected individuals where the privacy breach could reasonably be expected to result in significant harm to the individual, including:

- Identity theft or significant:
- Bodily harm
- Humiliation
- Damage to reputation or relationships
- Loss of employment, business, or professional opportunities
- Financial loss
- Negative impact on a credit record
- Damage to, or loss of, property

Notifying the Commissioner

The CIO must notify the Commissioner of privacy breaches that pose a reasonable expectation of significant harm. In circumstances involving significant harm where the individual is not notified (e.g., in

circumstances where notification could be reasonably expected to result in immediate and grave harm to the individual's safety or physical or mental health), public bodies must still notify the Commissioner.

Notifications to the Commissioner must be in writing and must contain the same information as the notification to affected individuals. They must also include an estimate of the number of affected individuals.

Exceptions to Notify

Regardless of whether significant harm may occur, notification is not required when it could be reasonably expected to:

- Result in immediate and grave harm to the individual's safety or physical or mental health; or
- Threaten another individual's safety or physical or mental health.