

Salt Spring Island Fire Protection District

POLICY MANUAL

Section	Information
Policy Number	AG-5302-01
Policy Title	Staff Requests for Access to Information

DEFINITIONS

“Administrator” as established in the *District’s “Officer Positions Establishment Bylaw No. 85.”*

“Agents” may include but are not limited to Contractors, sub-contractors, vendors, suppliers, or any other third-party individual directly or indirectly associated with the *District* in a business relationship.

“Board of Trustees” means the Board of Trustees of the Salt Spring Island Fire Protection District.

“Clients” means all persons or businesses receiving services from the *District* or their authorized or legal representatives.

“Collaboration Organization” means any agency with which the *District* is engaged in the delivery of a common or integrated program or activity.

“Confidentiality” is the responsibility and obligation of *staff* or *agents* of the *District* to ensure that the *Personal Information* or *Other Confidential Information* is kept secure and is collected, accessed, used, disclosed, stored and disposed of only for purposes necessary and authorized by the *District* or a *Collaboration Organization* to conduct its business.

“District” means the Salt Spring Island Fire Protection District.

“FIPPA” means the *Freedom of Information and Protection of Privacy Act [RSBC] Chapter 165.*

“FIPPA Coordinator” the person appointed by the *Board of Trustees* as the *Freedom of Information and Protection of Privacy Act* Officer for the *District*.

“Other Confidential Information” is the information provided to, collected or created by the *District* or a *Collaboration Organization*, which may or may not contain information on an identifiable individual, in the course of its business operations. Other Confidential Information includes:

- Information provided by an external vendor which, if disclosed would harm the business interests of the external vendor
- Information prepared as part of a pending or ongoing litigation, law enforcement, Internal Audit, Workers Compensation, Ombudsperson or Human Rights investigation
- In-camera deliberations of the *District*
- Unpublished statistical or intellectual property information related to organization initiatives may be disclosed pursuant to Part 2 of *FIPPA* unless one of the exceptions in Part 2 applies
- Information supplied in confidence to a mediator or arbitrator to resolve or investigate a labour relations dispute.

“Personal Information” means any information about an identifiable individual, but it does not include business contact information. Business contact information is information such as a person’s title, business telephone number, business address, email or facsimile number.

“Privacy Breaches” means the loss, theft, intentional or inadvertent unauthorized collection, use, disclosure, storage or disposal of personal information in the custody or control of the *District* or *Collaboration Organization*. Such activity is “unauthorized” if it occurs in contravention of Part 3 of the *Freedom of Information and Protection of Privacy Act* or this policy.

“Record” as defined in the *Freedom of Information and Protection of Privacy Act* includes books, documents, maps, drawings, photographs, letters, vouchers, papers and other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

“Staff” for purposes of this policy means members of the *Board of Trustees*, public members appointed to standing and select committees of the *Board of Trustees*,

employees (including Career, Administration and paid-on-call members), and volunteers engaged by the *District*.

POLICY OBJECTIVE

The Salt Spring Island Fire Protection District is a “public body” and therefore is required to comply with the *Freedom of Information and Protection of Privacy Act*.

In the legislation, Part 3 – Protection of Privacy , Division 1 details purposes for which *Personal Information* may be collected and Division 2 details use and disclosure of personal information by public bodies.

Section 30 of *FIPPA* requires a public body to make reasonable security arrangements to protect *Personal Information* in their custody or under their control. Section 33 prohibits the disclosure of *Personal Information* except as permitted by the legislation.

All *Agents* and other third parties, accessing or sharing *Personal Information* in the custody or control of the *District* must execute an agreement in which that party agrees to abide by the terms of a Privacy and Confidentiality agreement. Staff must take all reasonable steps to ensure *Agents* or third parties are not provided with access to records containing *Personal* or *Confidential Information*, except as permitted by this Policy and *FIPPA*.

Staff shall not make direct requests to other staff members for information or access privileges. All requests must be addressed to the Fire Chief, *Administrator* or *FIPPA Coordinator* as appropriate.

This access to information policy does not apply to Part 2 *FIPPA* requests.

Process for Requesting Access to Records that Contains or May Contain Personal and/or Confidential Information

Section 33.2 (c) of the *Freedom of Information and Protection of Privacy Act* only permits the disclosure of personal information within a public body to officers or employees of the public body for whom the information is necessary for the performance of their duties.

Staff who wishes to access records that may include *Personal* or *Confidential Information* to which they do not have “privileges or need to know” will make written

application to the *FIPPA Coordinator* on the form provided for this purpose identifying the information or records requested and explaining the rationale and purpose for the request. Prior “approval” of a request from a public member of a Board committee should be given by the Committee Chair. If a member of staff requests access to *Personal* or *Confidential Information*, other than to their own Employment Files, the request must be “approved” by the Fire Chief if it concerns an operational matter.

If the information is provided, the document(s) will be stamped “Confidential”, which means that the document(s) may be discussed only with other staff approved by the *FIPPA Coordinator* on the access request application. Confidential documents may be redacted if in the opinion of the *FIPPA Coordinator* there is no “need-to-know” and a *privacy breach* of the un-redacted information would harm a third party (a business or individual) or cause damage to the public reputation of the *District*.

If *Personal* or *Confidential Information* is provided to a trustee, all other trustees will be advised of the information provided. *Personal* or *Confidential Information* provided to members of a committee of the Board will also be copied to trustees.

If a request to access information in an Employment File(s) is approved, the *FIPPA Coordinator* may inform the employee(s) that their confidential records may be accessed along with the rationale for so doing. The employee may make a complaint to the Office of the Information and Privacy Commissioner if they question the legality of the disclosure.

If in the opinion of the *FIPPA Coordinator* the purpose for requesting the information is thought to be less than satisfactory the request may be declined with a written summary provided for the decision. Access to information requests may be deferred if there may be a contractual or legal obligation to obtain approval from a *Collaboration Organization* such as law enforcement or BC Emergency Health Services.

If a request for access to information from a trustee is declined by the *FIPPA Coordinator*, the matter may be referred to the *Board of Trustees* for a decision.

Process for Requesting Other Information

Staff requesting any record, other than records that may contain personal or confidential information should make their request directly to their supervisor who in turn will forward the request to the Fire Chief or Administrator as appropriate.

Other Staff requesting information, other than records that may contain personal or confidential information should make their request to:

- a) the Fire Chief when dealing with operation matters; and
- b) the *Administrator* when dealing with administration or financial matters.

Most *District* records will be routinely provided.

Should, in the opinion of either the Fire Chief or *Administrator*, the request for access to information requires more than an hour preparatory work, the request may not be actioned and, instead, referred to the *Board of Trustees* for direction.

Information provided may not be in a form acceptable for public scrutiny.

If a request is made in writing by a member of *staff* who is not acting in their professional capacity, but as a citizen, then it would be considered a valid access request under *FIPPA* and this policy would not apply.

Accuracy of Personal Information and Handling Requests for Correction of Personal Information

The *District* must make every reasonable effort to ensure that *Personal Information* that is collected is accurate and complete.

A *client* or staff member who believes that there is an error in their *Personal Information* may request correction of this information. Such a request must be considered by the *District*. If no correction or addition is made, the record must be annotated with the correction that was requested but not made.

BOARD DISCRETION

The provisions set out in this policy are subject to revision from time to time at the discretion of the *Board of Trustees*.

RELATED DOCUMENTS

Freedom of Information and Protection of Privacy Act [RSBC 1996] Chapter 165
Freedom of Information and Protection of Privacy Regulation B.C. Reg. 155/2012

APPROVALS

Access to Information Policy APPROVED

Approval date:		Approved by:	
1. Amendment date:	24 May 2018	Approved by:	
2. Amendment date:		Approved by:	
3. Amendment date:		Approved by:	