RECORDS INFORMATION MANAGEMENT RECORDS IN REGIONAL BOARD CUSTODY POLICY

Department	Administration	Policy No.	0340-95
Section	Records and Information Management	Date Approved by Board	
Repeals		Board Resolution #	

Amended		Board Resolution #	
Amended		Board Resolution #	
Amended		Board Resolution #	

Repealed		Board Resolution #	

1. Purpose

1.1 The purpose of the Records in Regional Board Custody Policy is to provide guidelines for the management of Peace River Regional District (PRRD) information assets which are in the custody of Regional Board members.

a) The *Freedom of Information and Protection of Privacy Act* (*FIPPA*) applies to all information assets under the custody or control of the PRRD. This includes any and all PRRD related email in the custody of a Regional Board member.

b) Using personal email accounts rather than PRRD specific email addresses to manage Regional Board communications may jeopardize the security, integrity and recoverability of information.

1.2 This policy encourages and assists Regional Board members with clear instructions to

a) Prevent the unintentional retention of PRRD records beyond prescribed timelines, thereby increasing the risks of information breaches and costs associated with Freedom of Information (FOI) requests and discovery of records during litigation.

b) Ensure PRRD records created or received by the Regional Board members are provided to the PRRD for proper records management and preservation.

c) Ensure records in the custody of Regional Board members are added to active PRRD files in a timely manner so decision making, FOI requests and litigation discoveries are based on complete, current and accurate information.

d) Ensure compliance with section 33.1 of the *Freedom of Information and Protection of Privacy Act* which makes it illegal for British Columbia's public bodies to store personal information outside of Canada without an approved Privacy Impact Assessment.

2. Scope

2.1 This policy applies to all PRRD records and information in the custody of PRRD Board members.

3. Definitions

3.1 See RIM-01 Records and Information Management Framework Policy for definitions.

4. Policy

4.1 Any PRRD records created or received by a Regional Board member must be provided to the Corporate Services Coordinator for proper records management.

a) Notes taken by a Regional Board member during a meeting are not PRRD records.
b) Any correspondence, including emails, that discuss the PRRD are PRRD records.

4.2 Compliance with 4.1 means that copies of the PRRD records in the custody of Regional Board members, once provided to the Corporate Services Coordinator are considered convenience copies (i.e., transitory records).

a) As transitory records, there is no need to file them or seek approval for destruction.
b) However, as with all potentially sensitive records, physical destruction requires bringing the physical records to the Corporate Services Coordinator for secure shredding.

4.3 Annually, Regional Board members shall destroy PRRD records older than 24 months.

a) Every year the Corporate Services Coordinator shall send an email to the Regional Board members instructing them to delete any PRRD records, physical or electronic, older than 24 months. Physical records shall be brought to the Corporate Services Coordinator for secure shredding.
b) Exceptions to this deadline may be allowed when tracking ongoing issues. Regional Board members will identify such exceptions and inform the Corporate Services Coordinator, who will track the issues.

4.4 PRRD records in the custody of a Regional Board member shall be protected according to the IT Acceptable Use and Info Security Policy 0340-001, including being protected by an anti-virus program acceptable to PRRD's IT department and being accessed only on a computer with a robust password.

4.5 Regional Board members shall not use non-PRRD email accounts when managing PRRD communications.

a) The Information Technology Manager will be responsible to:
    i. Issue PRRD email addresses to Regional Board members.
    ii. Ensure Regional Board members are competent in the use of the email accounts.
    iii. Inform Regional Board members of any associated risks.
    iv. Provide training to Regional Board members as necessary.

4.6 Regional Board members shall not store electronic records in a cloud-based internet site (e.g., OneDrive, Google, Dropbox, etc.) unless the site has been approved for use following completion of a Privacy Impact Assessment.

4.7 Texts, instant messages and social media contents are discoverable and may be obtained through FOI requests. The Director's Code of Conduct policy should be considered when posting or discussing any PRRD related information.

Affiliated Policies	Records and Information Management Accountability Policy 0340-88 Records and Information Management Policy 0340-89 Vital Records Policy 0340-92 Privacy Management Program Policy
Affiliated Procedure	