RFA BANK OF CANADA

Privacy Policy

Board Approval: July 2023

NFRGC Review: June 2023

Policy Owner: Chief Privacy Officer
Version # 3.0

TABLE OF CONTENTS

1. Purpose

This Policy sets out the principles that govern how RFA Bank of Canada ('RFA' or "the Bank') manages Personal Information.

2. Scope & Applicability

RFA is responsible for Personal Information that it collects or controls about its customers, employees, and certain other people. This Policy applies to RFA's directors, officers, employees, and anyone with whom we share Personal Information whenever they handle Personal Information for which RFA is responsible.

3. Definitions

Personal Information means information about an identifiable individual which is governed by applicable privacy legislation in Canada such as PIPEDA and similar provincial legislation listed below. This includes, for example,

- Social Insurance Numbers;
- Financial Information;
- Personal (but not business) contact information; and,
- Employment Information,

PIPEDA means the Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5

4. Principles

We adhere to the following ten fair information principles set out by the Office of the Privacy Commissioner:

4.1 Accountability

We are responsible for Personal Information under our control. We appoint an individual to act as Chief Privacy Officer to be accountable for our compliance with these fair information principles. The Chief Privacy Officer, overseen by the Board of Directors, maintains and oversees the Bank's adherence to a privacy framework that incorporates these principles. The privacy framework includes this Policy and a set of standards and procedures that set out how we implement it.

4.2 Transparency of Purpose

We tell people the purposes for which we collect their Personal Information when or before we collect it. For example, we may collect Personal Information about our customers to:

- verify their identity;
- determine whether our products are suitable for their circumstances;
- understand and manage our risks, including credit and other risks;
- comply with legal and regulatory requirements;
- enable us and our servicers to communicate with them; and,
- ensure that the information we have is up-to-date before we use it.

4.3 Consent

We do not collect, use, or keep Personal Information about anyone unless they have given us their informed consent to do so. By "informed consent", we mean that we have explained to them what information we collect, what we use it for, how long we keep it, and how we protect it. Individuals have the right to withdraw their consent, subject to legal or contractual restrictions and on the understanding that we may not be able to continue to provide services if we do not have the information we need for that purpose.

4.4 Limited Collection

We collect only the Personal Information that we need for the purposes for which we told people we would use it, and we only collect it by fair and lawful means. These may include obtaining information from third parties such as credit reporting agencies and other sources of information that are available to help us satisfy our legal obligations and manage our risk.

4.5 Limited Use, Disclosure, and Retention

We only use, disclose, or keep information for the purposes for which we told people we would use it when we collected it. We do not sell Personal Information, but may disclose Personal Information to other companies that we work with, such as credit rating agencies, mortgage servicing companies, and GIC brokers. When we share Personal Information with such third-parties, we ensure that they are subject to strict privacy controls, including this Policy, and that they maintain proper accountability and security measures to protect the Personal Information that we share with them. We maintain a data retention standard that sets out how long we and those with whom we share it keep various kinds of information. Generally, for Personal Information collected in relation to our provision of mortgages or GICs this is seven years after the end of the term of the mortgage or GIC. In certain cases, we may retain information for longer periods, usually for legal reasons.

4.6 Accuracy

We ensure that Personal Information is as accurate, complete, and up-to-date as required to properly satisfy the purposes for which we are using it. We do this by confirming information we receive, cross-checking it with other information sources, and updating it before using it again if some time has passed since we obtained it. We do not contact customers unnecessarily to update information that we do not need to use for a purpose that we have disclosed.

4.7 Security Safeguards

We use appropriate physical, technical, and procedural means to protect the security of Personal Information for which we are responsible. This includes limiting access to our premises where we keep the information, encrypting Personal Information both at rest and in transit, employing industry-standard anti-virus technologies, and maintaining and implementing a formal privacy framework. We ensure that all our staff receive regularly updated training on how to handle Personal Information according to this Policy and the law. We also ensure that those with whom we share Personal Information employ similar safeguards and we regularly confirm that they continue to do so as long as they have access to the Personal Information for which RFA is responsible.

4.8 Policy & Practice Transparency

We make information about our Personal Information policies and practices publicly and readily available. This includes posting this Policy publicly on our website and making it and the detailed Standards and Procedures that go with it available to individuals on request.

4.9 Accessibility & Correctability

We give people access to the Personal Information that we have about them when they ask for it by publishing this Policy and the Chief Privacy Officer's contact information on our website and including it in our disclosure packages. After we first ascertain the identity of the person requesting the information (or

in the case of persons requesting information about other people, ascertaining that they have proper authority to receive it) we tell them what information we have, and how we use and disclose it to enable them to correct any errors or omissions.

4.10 Openness to Challenge

We enable people to contact our Chief Privacy Officer to challenge our compliance with these principles. The Chief Privacy Officer responds to all such challenges in a timely and appropriately detailed manner.

4.11 Risk Appetite & Exceptions

RFA's Risk Appetite Framework establishes limits regarding the level of risk that the Bank is willing to accept and forms the basis for this Policy. The Bank has a low risk appetite for breaches of and exceptions to this Privacy Policy. Accordingly, exceptions may only be granted in writing by the Chief Privacy Officer in consultation with the Chief Risk Officer. Exceptions are granted only in unusual circumstances (such as in the case of confidential investigations, or legally compelled disclosure). The Chief Privacy Officer maintains a record of all exceptions together with written rationales for each and reports them to the Governance, Conduct Review, and Compensation Committee quarterly. All incidents of non-compliance with this Policy that are not the subject of a written exception are considered policy breaches and are reported as such.

5. Policy Requirements

5.1 Standards and Procedures

The Chief Privacy Officer maintains Standards and Procedures that specify how each of the foregoing Fair Privacy Principles are to be implemented at RFA. The Privacy Standards and Procedures are reviewed at least annually and approved by management at the Non-Financial Risk and Governance Committee. Pursuant to principle 3.8 above, we publish this Policy on RFA's website and we make the Standards and Procedures available to the public on request.

5.2 Relevant Regulatory Requirements and Guidance

The following legislation and official guidance govern this policy and inform the Standards and Procedures RFA follows to implement the Fair Information Principles

- *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("PIPEDA"): https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/FullText.html
- Privacy Guidance from the Office of the Privacy Commissioner of Canada: https://priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/
- *Personal Information Protection Act*, SA 2003, c P-6.5 ("Alberta PIPA"): https://www.canlii.org/en/ab/laws/stat/s a-2003-c-p-6.5/latest/sa-2003-c-p-6.5.html
- *Personal Information Protection Act*, SBC 2003, c 63 ("BC PIPA"): https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00_03063_01
- *An Act Respecting the Protection of Personal Information in the Private Sector*, SQ 1993, c P-39.1 ("Quebec Act"): https://www.legisquebec.gouv.qc.ca/en/document/cs/p-39.1

6. Roles and Responsibilities

The Board of Directors, supported by the Governance, Conduct Review, and Compensation Committee:

- oversees the Bank's practices and procedures for compliance with privacy laws and the protection of employee' and customer's personal information;
- reviews and approves this Privacy Policy in accordance with the Board Policy Review Schedule;
- approves the appointment and removal of the Chief Privacy Officer; and,
- oversees and advises management and the Chief Privacy Officer on matters related to this Policy.

The Non-Financial Risk & Governance Committee of management

- reviews and recommends changes to this Policy to the Board of Directors;
- reviews and approves Privacy Standards; and,
- reviews Chief Risk Officer and Chief Privacy Officer reports of privacy incidents.

The Chief Privacy Officer

fulfils the obligations set out in the Chief Privacy Officer's Mandate as approved by the Board of Directors, including:

- providing strategic advice to management and employees regarding privacy matters;
- maintaining knowledge of relevant laws and regulations applicable to all lines of business;
- establishing, documenting, and communicating privacy-related standards, policies, procedures, and internal controls;
- ensuring that those to whom this Policy applies understand and fulfil their responsibilities for complying with it;
- monitors and reports on adherence to this Privacy Policy and to the Privacy Standards and Procedures by RFA and, as part of the Third-Party Risk Management Program, by third parties with whom RFA shares Personal Information; and,
- responding to, and reporting on privacy incidents, and enquiries, including reporting to Privacy regulators such as the Office of the Privacy Commissioner as required.

Third-Party Risk Management

- provides oversight of third-party vendors via the Third-Party Risk Management Program, including working with the Chief Privacy Officer to monitor third-parties' compliance with privacy obligations

Management & Employees of RFA

- promote a culture of concern for privacy and compliance with the fair information principles;
- implement the fair information principles in their handling of Personal Information in accordance with this Policy and the Privacy Standards and Procedures; and,
- report privacy incidents or concerns to the Chief Privacy Officer and assist in their resolution.

Internal Audit

- provides internally independent assurance regarding privacy risk management.

7. Monitoring & Reporting

The Chief Privacy Officer reports to the Non-Financial Risk and Governance Committee of Management and to the Governance, Conduct Review, and Compensation Committee of the Board on the evolution of applicable privacy law, on RFA's compliance with this Policy, and on any privacy incidents or concerns together with plans to address them.

Report	*Preparer*	*Audience*	*Frequency*	*Description*
Policy Exceptions and Breaches	CPO	GCRCC	As required	• Material exceptions to or breaches of this Policy.
Privacy Report			Quarterly	• Accepted exceptions to this Policy during the quarter. • Complaints and incidents of non-compliance with this Policy during the quarter and plans to address them. • Anticipated changes to applicable privacy laws or industry standards.
Attestation			Annually	• Management and employees attest that they have reviewed and adhered to this policy. • CPO attests that a Privacy Risk and Control Assessment has been conducted and that the Bank is in compliance with its Privacy obligations.

8. Record Keeping

The CPO will retain records of all exceptions and incidents related to this Policy in accordance with the Bank's records retention schedule.

9. Oversight & Authority

9.1 Ownership & Approval

This Policy is owned by the Chief Privacy Officer and approved by the Board.

9.2 Policy Compliance and Exception Management

The Chief Privacy Officer is responsible for overseeing compliance with this Policy and for reporting non-compliance to the Chief Risk Officer and the Chief Executive Officer. Failure to comply with this policy on the part of Bank employees may be grounds for disciplinary action up to and including termination of employment.

Exceptions to this must be documented and approved by the Chief Risk Officer. The Chief Risk Officer and the Chief Privacy Officer will provide a summary of the exceptions that have been granted in each quarter to the Chief Executive Officer and the Board of Directors. Exceptions will be reviewed periodically and will not be renewed automatically. Documentation of the exceptions will include:

- the reasons for the exception;
- an analysis of the risks associated with the exception;
- compensating controls to mitigate such risks; and,
- plans to remedy any deficiencies, if applicable.

9.3 Policy Review

This policy will be reviewed periodically according to the Board policy review schedule. The review is completed to ensure that the Policy remains consistent with business strategy, internal practices, industry practices, and applicable legal and regulatory requirements.

10. Change Log

Version	Approval Date	Made By	Description	Approved By
1.0	July 2021	CPO + Tech Ops	New policy based on the former Information Security and Privacy Policy. The IT Information Security specifics were moved to the Information Technology and Security policy. A reconciliation of the topics and movement has been performed to ensure completeness.	BOD
2.0	Nov 2022	CPO	As a result of the annual policy review, the Privacy Policy was reduced in length and updated to reflect the governance and removed any Information Security and Technology Policy requirements.	BOD
3.0	Jul 2023	CPO	Policy further simplified and revised to reflect key principles and required policy elements; most detail re implementation referred to Standards and Procedures document.	BOD