DUCA IMPACT LAB PRIVACY POLICY

DUCA Impact Lab

POLICY REVISION & UPDATE CHART

Date	Description of Revision/Update	Version	Author/ Reviser/ Reviewer	Approved by	Board Approval Date
12/17/2020	New Policy Created	1.0	Keith Taylor		
06/29/2021	Final Draft Created	1.1	Keith Taylor	Board Vote	August 9, 2021

Privacy Policy Table of Contents

Contents

PRIVACY POLICY

This Board policy addresses the DUCA Impact Lab's approach to the handling of personal information as required by the federal act concerning privacy.

1.1 DEFINITIONS

The **Charity** refers to the DUCA Impact Lab

The **Corporation** refers to the DUCA Impact Lab Social Finance Corporation

The **Act** refers to the Personal Information Protection and Electronic Documents Act (PIPEDA)

ED refers to the Executive Director, DUCA Impact Lab

The Board refers to the DUCA Impact Lab Board of Directors

The term **Data** refers to personal information collected about borrowers in the DUCA Impact Lab Social Finance Corporation loan pilots, from partners working on DUCA Impact Lab initiatives or programs, or from donors supporting the work of the charity.

Related Entities refers to the DUCA Impact Lab Charity, or organizations that the charity has a controlling interest in.

The term **Stakeholder** refers to borrowers, donors and partners participating in, supporting, or contributing to DUCA Impact Lab or DUCA Impact Lab Social Finance Corporation activities.

1.2 SCOPE

The guidelines outlined in this policy apply to the DUCA Impact Lab and the DUCA Impact Lab Social Finance Corporation.

1.3 OBJECTIVES

The policy outlined in this document seeks to achieve the following objectives:

- Establish a clear framework for management decision making pertaining to borrower and partner data in the DUCA Impact Lab Social Finance Corporation loan pilots
- Ensure personal information is protected and collected transparently and with purpose
- Define the rights of pilot program borrowers and donors to the DUCA Impact Lab Charity to access data and under what circumstances it will be shared
- Ensure alignment with privacy legislation applicable to commercial activities conducted in charitable organizations

1.4 PROTECTION OF PERSONAL INFORMATION

The DUCA Impact Lab has aligned its privacy policy with the *Personal Information Protection and Electronic Documents Act ("Act")*. The following principles form the basis of the act and guide the approach at the DUCA Impact Lab and its related entities:

i. **Accountability** – The charity and corporation are responsible for personal information under its control and shall designate a Privacy Officer who is accountable for compliance with the act.

ii. **Identifying Purposes** – The purposes for which personal information is collected shall be identified by the charity and corporation at or before the time the information is collected.

iii. **Consent** – The knowledge and consent of the individual providing the information is required for the collection, use and disclosure of personal information, except in specific circumstances as described within this policy.

iv. **Limiting Collection** – The collection of personal information shall be limited to that which is necessary for the purposes identified by the charity and the corporation. Information shall be collected by fair and lawful means.

v. **Limiting Use, Disclosure and Retention** – Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the Member or as required by law. Personal information shall be retained only if necessary, for the fulfillment of those purposes.

vi. **Accuracy** – Personal information shall be as accurate, complete, and up to date as is necessary for the purposes for which it is to be used.

vii. **Safeguards** – Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. The charity and the corporation will apply the same standard of care as it applies to safeguard its own confidential information of a similar nature.

viii. **Openness** – The charity and the corporation shall make readily available to stakeholders specific, understandable information about its policies and practices relating to the management of personal information.

ix. **Individual Access** – Upon request, a consenting individual shall be informed of the existence, use, and disclosure of their personal information, and shall be given access to that information. An individual providing information is entitled to question the accuracy and completeness of the information and have it amended as appropriate on proof of inaccuracy.

x. **Challenging Compliance** – An individual providing information shall be able to address questions regarding compliance with the above principles to the Privacy Officer. Where an inquiry is made, the inquiry will be directed to the Privacy Officer to respond.

1.5 ACCOUNTABILITY

The Board of Directors ("Board") is accountable for the charity and the corporation's compliance with the act, the creation and review of all Board policies specific to the act and the designation of a Privacy Officer. The ED will serve as the DUCA Impact Lab Privacy Officer under this policy and will have primary day-to-day responsibility for compliance.

1.6 IDENTIFYING PURPOSES FOR USE OF PERSONAL INFORMATION

1.6.1 Approval and Documentation of Purposes

The Privacy Officer will ensure documentation exists to outline all purposes, including existing and new purposes, for which personal information is collected, used, or disclosed. All new purposes must be approved by the Privacy Officer prior to collection of information for the new purpose.

If the proposed purpose is significantly different than existing purposes or involves a new disclosure to a third party, the proposed purpose must be approved by the Privacy Officer prior to implementation.

1.6.2 Disclosure

The Privacy Officer will make reasonable efforts to ensure that all individuals sharing information with the charity and/or the corporation are aware of the purpose for which their personal information is collected, including any disclosure of their personal information to third parties. The primary communication method will be the use of written or electronic statements on applications, forms, contracts, and agreements.

1.7 CONSENT FOR PERSONAL INFORMATION

Consent will be obtained at the time the information is shared with the charity and/or the corporation. Once consent is obtained, further consent will not be required when personal information is supplied to agents and partners of the DUCA Impact Lab who carry out functions such as data processing, credit bureau reporting, impact analysis and other research activities.

The Privacy Officer must authorize all instances where information is collected, used, or disclosed without stakeholder's knowledge and consent.

1.7.1 Obtaining Consent

Express consent in writing, using applications, signed forms and contracts, will be used for obtaining consent for the collection, use or disclosure of personal information.

The Privacy Officer must review and approve all methods of obtaining consent.

1.7.2 Limits on Consent to Information Collection

Information will not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill explicitly specified and legitimate purposes.

The Privacy Officer will review the personal information requirements of all products or services to ensure that only information required for the legitimate purpose is collected and used.

1.7.3 Withdrawing Consent

The charity and/or corporation will obtain a written request (signed and dated) from a stakeholder who seeks to withdraw consent. The written request must acknowledge that the stakeholder has been advised that they may subsequently not be able to access the related product, service, or information.

The withdrawal of consent is subject to any legal or contractual restrictions that may exist with other organizations such as: The Income Tax Act; credit reporting; or to fulfill other fiduciary or legal responsibilities.

1.8 LIMITING COLLECTION OF PERSONAL INFORMATION

The charity and the corporation will only collect personal information that is necessary as part of the normal course of serving a stakeholder, as well as to administer the business, including:

a) To protect against fraud and error
b) To comply with applicable laws and regulatory requirements
c) To manage and assess risks, operations, and relationships
d) To evaluate impact and support research objections related to the mission of the charity and/or corporation; and
e) To improve and develop products and services

1.9 LIMITING USE, DISCLOSURE AND RETENTION OF PERSONAL INFORMATION

1.9.1 Safeguard Standards

The Charity and/or the Corporation will protect the interests of its stakeholders by taking reasonable steps to ensure that:

A) Government agency and law enforcement orders or demands comply with the laws under which they were issued
B) Only personal information that is legally required is disclosed
C) Due diligence is conducted on vendors to ensure that all information disclosed to third parties receives the same standards of care as within the charity and/or corporation
D) Suppliers, agents, and third parties are only provided the information needed to perform the services, as outlined in formal contracts
E) Employees only access data that is necessary for them to fulfill their role and responsibilities

The charity and/or corporation will make reasonable attempts to notify the stakeholder that an order has been received if the law allows. Notification may be by telephone, or by letter to the stakeholder's address.

1.9.2 Retention & Destruction of Personal Information

The Privacy Officer will ensure that guidelines and procedures with respect to the retention of personal information are maintained within the charity and/or corporation. The Privacy Officer will ensure that guidelines and procedures are in place to govern the destruction of personal information.

1.10 ACCURACY OF DATA

The Privacy Officer will ensure guidelines and procedures are in place to ensure stakeholder data is as accurate, complete, and current, as necessary. The charity and/or corporation will not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

1.11 SAFEGUARDS OVER PERSONAL INFORMATION

The charity and corporation security safeguards will protect personal information against loss or theft, as well as unauthorized access, use, copying, modification, disclosure, or disposal.

The Privacy Officer will conduct regular reviews of organizational practices related to the safeguarding of personal information

1.11.1 Destruction of Personal Information Safeguards

The charity and the corporation will destroy personal information in a secure manner to prevent any unauthorized access.

1.12 INDIVIDUAL ACCESS TO PERSONAL INFORMATION

All requests for access to personal information must be submitted in writing and include adequate proof of the individual's identity/right to access, and sufficient information to allow the credit union to locate the requested information.

1.12.1 Restricting Access

Exceptions to the access requirement will be limited and specific and include the following:

a) Providing access would reveal personal information about a third party
b) Information protected by solicitor-client privilege
c) Providing access would reveal confidential commercial information
d) Providing access might threaten the life or security of another individual
e) Information generated during a formal dispute resolution process
f) Personal information to which the stakeholder has requested access has been requested by a government institution for law enforcement, or an investigation related to law enforcement
g) Information collected without knowledge or consent for purposes related to investigating a breach of an agreement or a contravention of Ontario or Canadian law

The Privacy Officer must be made aware of any situations involving employees, Members or other individuals that would result in legal restrictions on access.

1.12.2 Response Time

The charity and/or the Corporation will respond to a stakeholder's request for information within 30 days. This timeframe can be expanded, but only if required, and on written notification to the stakeholder.

1.13 PROTECTION OF MEMBER INFORMATION WITH THIRD PARTIES

1.13.1 Third Party Accountability

The Charity and/or the Corporation will use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. The Privacy Officer must be satisfied that the personal information is adequately safeguarded by the third party.

1.13.2 Third Party Agents/ Suppliers/DUCA Impact Lab Pilot Partner Safeguards

Third party agents or suppliers will be required to safeguard personal information disclosed to them in a manner consistent with the policies of the DUCA Impact Lab. Neither the Charity or Corporation will enter any commercial relationships with organizations that do not agree to abide by acceptable limitations on information uses and appropriate safeguards.

1.14 BREACH NOTIFICATION PROVISIONS

Under Canada's new Privacy Breach Notification Rules, The DUCA Impact Lab is required to notify individuals and report to the Office of the Privacy Commissioner ("OPCC"), all breaches where it is reasonable to believe that the breach constitutes a "real risk of significant harm to the individual".

The term ‘significant harm’ includes, but is not limited to, humiliation, damage to a reputation or relationship, and/or identity theft. The term ‘real risk’ requires consideration of various factors, such as the sensitivity of the information, the probability of misuse, and any other prescribed factor.

The notice provided to individuals must be given as soon as feasible and must contain sufficient information to allow the individual to understand the significance of the breach, and to take steps, if possible, to reduce the risk of harm. The OPCC may publish information about notices if it is determined that it would be in the public interest to do so. Section 10.2 of PIPEDA requires organizations to notify other organization and government institutions, without requiring consent, if such notice could reduce risks or mitigate harm.

1.15 BOARD REPORTING AND NOTIFICATION

Quarterly Reporting

The Privacy Officer will continually review compliance within the charity, corporation and third party suppliers, and will report to the Board as needed, any matters concerning non-compliance with the principles, policies or procedures that are likely to require input from the Board (e.g., any matter that could result in an investigation or audit by the Office of the Privacy Commissioner).