TORONTO GRANTS, REBATES, AND INCENTIVES PORTAL (TGRIP)

User Guide for Organizations

Access TGRIP at: https://cot.smartsimple.ca

DEFINITIONS

Acronym / Term	Definition
TGRIP	Toronto Grants, Rebates, and Incentives Portal
SmartSimple	Underlying cloud system supporting TGRIP
Docusign	Third-party application for signature collection

GETTING STARTED

To apply for grants, rebates or incentives in TGRIP, you must:

1. Register/Login. You will receive an email from support@smartsimple.ca containing a link to TGRIP where you will be asked to personalize your password. If the link has expired, select ***FORGOT PASSWORD?*** on the TGRIP home page to receive another email.

2. Complete an Organization Profile. This contains general organization information accessible to City staff in multiple divisions.

3. Access funding opportunities to apply.

CONTACT INFORMATION

For technical issues, contact the TGRIP Central Support Team at TGRIP@toronto.ca A staff member will respond within two business days.

For issues relating to a funding opportunity or a current grant, rebate or incentive, refer to the funding opportunity guidelines and contact the lead City staff for the project.

Users cannot see any Application or its components (e.g., Reports) unless they are added to the application's Contact list

***go to section*: ASSIGNING AND ADDING STAFF TO APPLICATIONS**

WELCOME EMAIL

Once your account has been created in TGRIP, the system will send you a welcome message with a link and instructions to set your password. The Welcome Email link expires in 48 hours.

To request a new activation link, select ***FORGOT PASSWORD?*** on the TGRIP home page.

WHITELIST TGRIP EMAILS

If your organization is not receiving emails from TGRIP, ask your organization's IT Support Team to "whitelist" TGRIP emails.

A whitelist is a list of emails to always be considered safe and not spam. Spam filters often include the ability to "whitelist" certain sender addresses, email addresses, or domain names to stop those emails from being rejected or sent to a junk mail folder. It is highly recommended that users whitelist TGRIP and Docusign to ensure email notifications are received in a timely manner.

Emails from TGRIP and Docusign and will have the following details:

TGRIP No Reply	TGRIPnoreply@smartsimple.com
TGRIP Central Support Team	TGRIP@toronto.ca
Docusign via Docusign	dse@camail.docusign.net

The City of Toronto is not responsible for the content of websites we do not manage or own.

wikiHow article: How to Whitelist an Email: Gmail, Outlook, Yahoo, more

NAVIGATION AND SEARCH

NAVIGATION

To move backwards to previous screens, select the back arrow, or dropdown arrow, below the header. All pages viewed in the current session can be accessed.

Do not use your browser's back button.

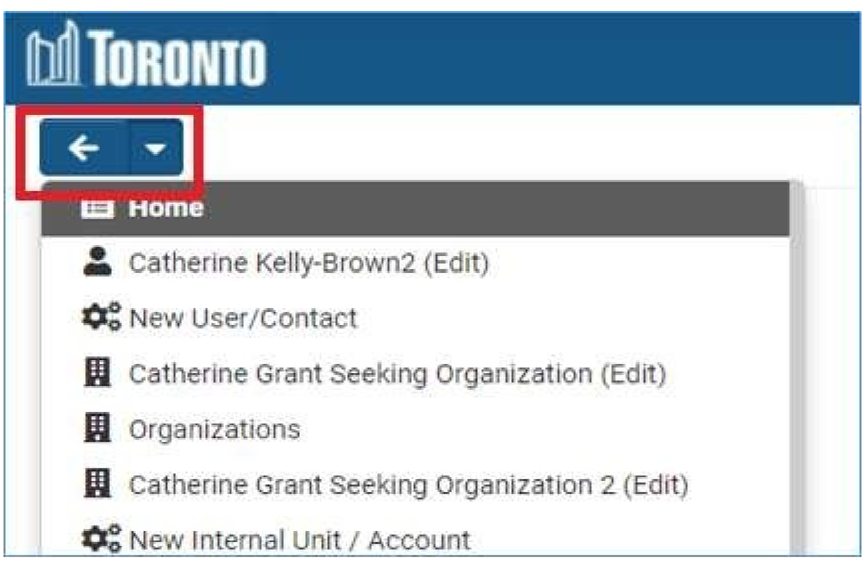


Figure 1 navigation BACK arrow

SEARCH

From any screen with a search input field, the text entered will be searched throughout the titles and descriptions and is not case-sensitive. For example, "cath" would return "***Cath***_erine_", "_Toronto_ ***Cath***_olic School Board_", and "***Cath***_edral Park_".

Previous search terms will be saved and pre-populated the next time the same screen is opened.

LOGIN

ORGANIZATION ACCOUNT

An organization's account allows access, at any time, to all the applications, agreements, and reports that organization staff have saved or submitted in TGRIP. There can only be one account for each organization, which can have multiple people within it.

A Contact is a person associated to the organization. The organization has complete control over who gets access to the organization’s account and applications. The organization can add or de-activate a Contact at any time. Contacts cannot be deleted.

LOGGING INTO AN ACCOUNT

Log in to your account by navigating to the TGRIP home page: http://cot.smartsimple.ca/

Your email address is your username on the system. The system will only allow for unique email addresses. Do not use general email addresses (e.g., info@[your org].ca) as more than one person may be able to use it significantly reducing security and auditing capabilities.

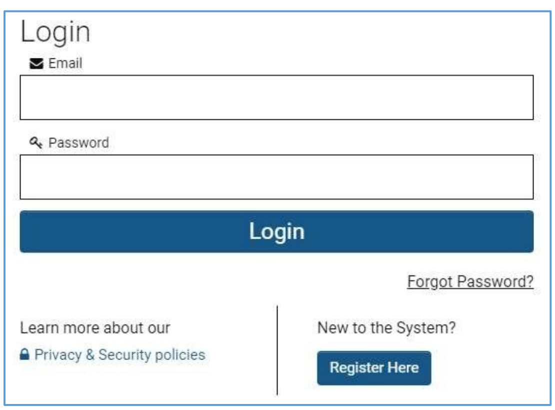


Figure 1: TGRIP login screen

1. Input your email address in the ***Email*** field
2. Input your password in the ***Password*** field. Select the eye symbol to display characters typed in this field.
3. Select the ***Login*** button
4. Follow the MFA (Multi-Factor Authentication) instructions to submit your verification code

TROUBLESHOOTING LOGINS

If you are not receiving Multi-Factor Authentication (MFA) emails with your verification code to login, check all of your e-mail spam/junk, deleted/trash/bin, and Inbox folders.

- MFA emails are sent from *TGRIP No Reply TGRIPnoreply@smartsimplemailer.com* and should arrive within 6 minutes.
- Confirm you did not accidentally block emails sent from TGRIP to your personal account.
- If you share an email with others, confirm they have not set-up rules that are applied when emails arrive nor disposed of the MFA email.
- Confirm that your Login Access is set to "*User Access*" in your TGRIP Organization Profile's Contacts list.
- Confirm that your IT Team has added smartsimple.com and smartsimplemailer.com to your whitelist and to your personal email program.

CHANGING YOUR PASSWORD

TGRIP passwords must be changed every 90 days. This requirement cannot be removed.

Passwords must have a minimum of 12 characters, cannot be reused, and must include at least:

- one uppercase letter,
- one lowercase letter,
- one number, and
- one symbol ~ ! @ # $ % ^ & * ( ) { } [ ] ; : ' " < > ?

CHANGING YOUR PASSWORD WHEN REGISTERING

Select the ***Set Password*** link in the welcome email

CHANGING YOUR PASSWORD AFTER ACCOUNT IS CREATED

1. Select ***Update Password*** from the top menu

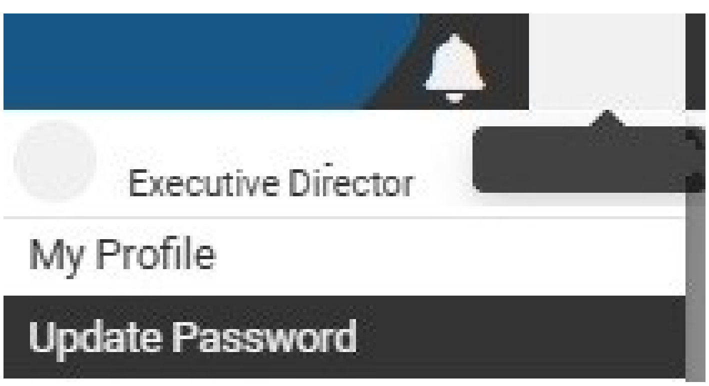


Figure 2 Update Password menu item

2. Enter current password
3. Enter new password, twice
4. Select ***SAVE***

Passwords are case sensitive and are subject to rules that are intended to strengthen security.

Take all reasonable measures to:

- protect your security in the online system including, but not limited to, refraining from sharing your password
- prevent the loss, disclosure, modification, and unauthorized use of your password
- control access to computers or devices containing your password.

You must notify your organization's primary contact immediately if you have any reason to believe that your TGRIP username and password have been compromised or are considered insecure.

FORGOTTEN PASSWORD

You can reset your password at any time by selecting the ***Forgot Password?*** link found on the TGRIP home page and following its instructions.

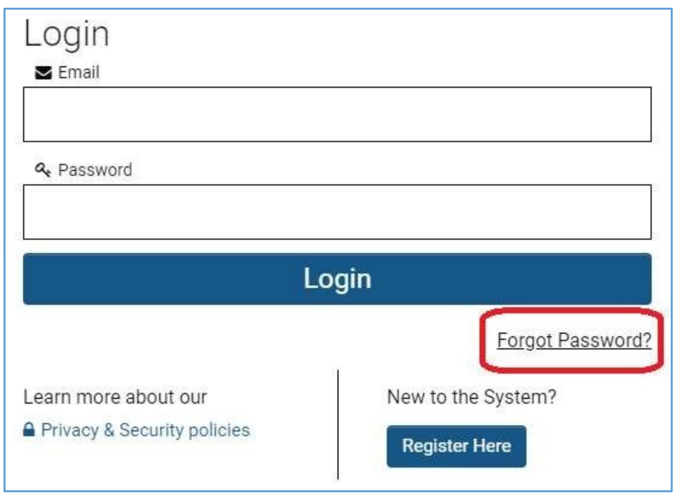


Figure 3 TGRIP login page showing the location of the "Forgot Password?" link

CONTACTS, ROLES, AND PERMISSIONS

CREATING CONTACTS AND ASSIGNING ROLES

Contacts can be added by selecting the menu links for ***Organization Profile***, then ***Contacts***, then ***New***, and finally ***New Contact***.

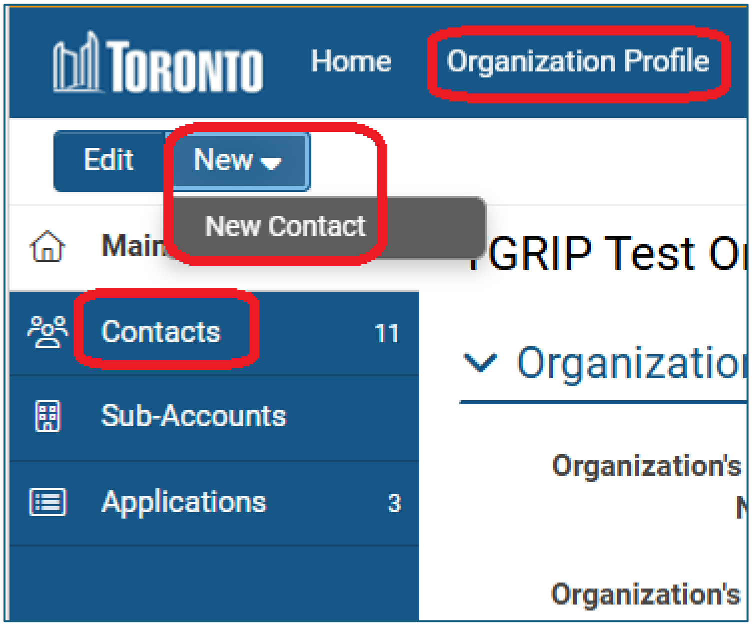


Figure 4 menu links to add a new contact

Assign an Applicant role, enter all contact details, then select ***Update Account***. The system will send an email to the contact's email address with a time-limited link to activate their TGRIP account. If it has expired before use, the link can be requested again by selecting ***FORGOT PASSWORD?*** on the home page.

Repeat these steps for each person who will need access to TGRIP to complete your organization's applications or reports.

If a member of your organization already has an account in TGRIP, or works with more than one organization, you must contact TGRIP@toronto.ca to assist you.

CHANGE OR DEACTIVATE CONTACTS IN ORGANIZATION

1. Select ***Organization Profile***

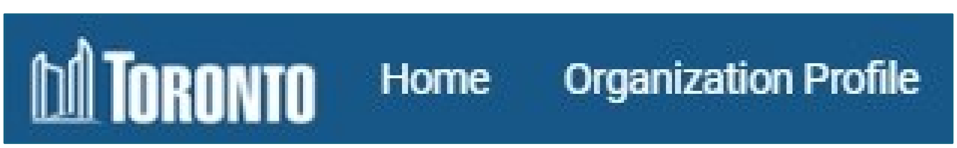


Figure 5 Organization Profile link

2. Select ***Contacts*** menu item
3. Select the person you need to update
4. Complete changes or select ***Actions*** then ***Disable Login Access***
5. Select ***Update Account*** /***Save***

ORGANIZATION PROFILE

The Organization Profile includes organization-level information and documents. It can be updated at any time. Its profile is automatically attached to all applications you submit through TGRIP.

Each organization will have only one Organization Profile. Some large organizations have multiple sites, multiple business streams, and have multiple profiles on 211.ca; however, if they are under one organization umbrella or governed by one Board of Directors, they can only have one Organization Profile.

COMPLETING THE ORGANIZATION PROFILE

To access your organization profile, select ***Organization Profile***. The Organization Profile is organized by categorical tabs.

- Contact Info
    - organization's head office location details, registered email domain
- Organization Info
    - date established, mission statement, organization type, sector profile, staffing
- Service Locations
    - area(s) of the city where core services and programs are provided
- Core Work
    - general and core programs and services
- Demographics
    - population groups that are the focus of core programs and services
- Governance (for Incorporated entities)
    - Annual General Meeting details, list of the Board of Directors
- Leadership (for non-incorporated entities such as Grassroots and Resident-Led)
    - list of leadership persons
- Documents
    - organization-level documents such as Declaration of Non-Discrimination, insurance certificates, bylaws, Complaint Policy, Audited Financial Statements
- Financials
    - generate a Payment Confirmation Letter

1. Select ***Organization Profile***
2. Complete all mandatory fields marked with an asterisk *
3. Complete any optional fields as needed or relevant
4. Select ***Save Draft*** to save details until ready to submit
5. Select ***Submit*** when all information is complete

UPDATING THE ORGANIZATION PROFILE

If changes to the Organization Profile are needed after submission, it needs to be changed back to “Draft” status. Please contact TGRIP@toronto.ca for assistance. Once updates have been completed, select ***Submit*** to return the Organization Profile to submitted status.

FINDING A FUNDING OPPORTUNITY

Funding Opportunities currently accepting applications are found on the home page. Select the ***My Funding Opportunities*** tile to view and/or apply.

For each funding opportunity, the deadline date and end time are indicated. There is also a link to the corresponding funding guidelines. To access the application, select the ***View Details/Apply*** button.

Each application is unique to the funding opportunity. Please consult its guidelines for application requirements, timelines, and grant staff contact information.

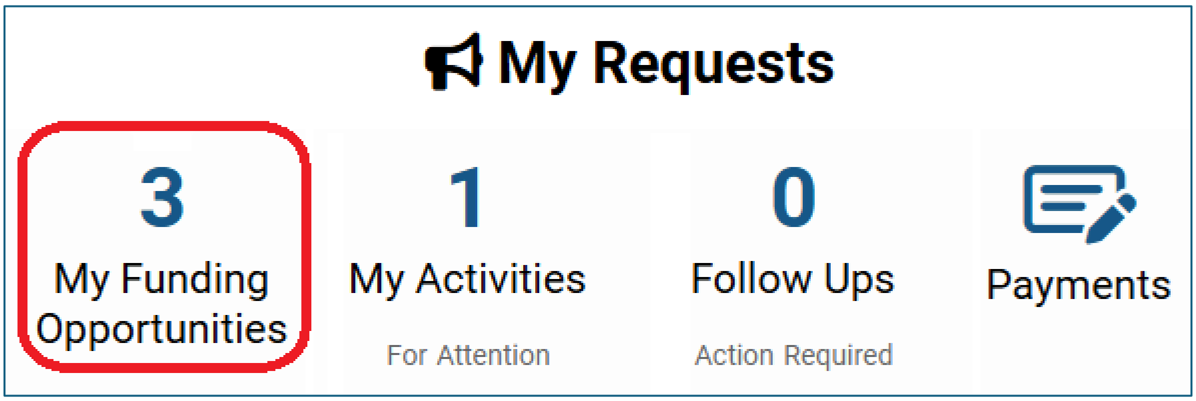


Figure 6 My Funding Opportunities home page tile

SUBMIT AN APPLICATION

1. Select ***My Funding Opportunities*** on the main page (reference: *Figure 6 My Funding Opportunities home page tile*)
2. Select a Funding Opportunity
3. Complete all areas within the various tabs of the application
4. Select ***Save Draft*** to save information while working or to complete in multiple sessions
5. Select ***Validate*** to confirm all necessary details have been entered
    a. Action any items listed in the validation area
    b. You will not be able to submit until errors and warnings have been addressed
6. Select ***Submit*** to submit application
7. Select ***Withdraw*** if you no longer wish to apply

VIEWING APPLICATIONS AND REPORTS

APPLICATIONS

Applications are accessed from the home page.

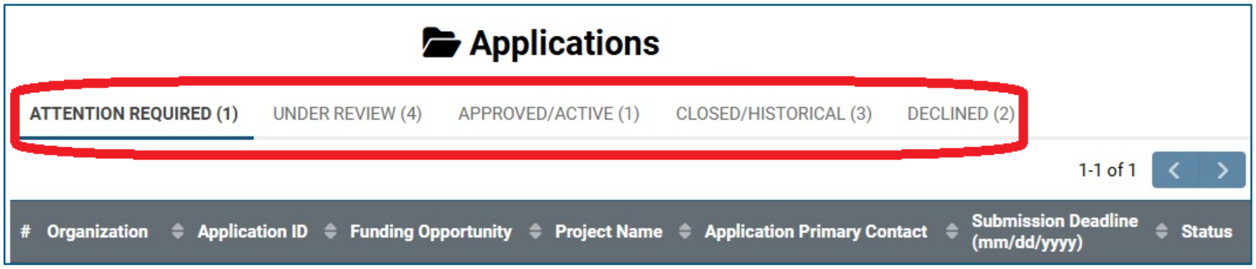


Figure 7 Application lists on home page

Applications are organized within one of multiple tabs, based on their current status. The number on the tab indicates the number of applications it holds.

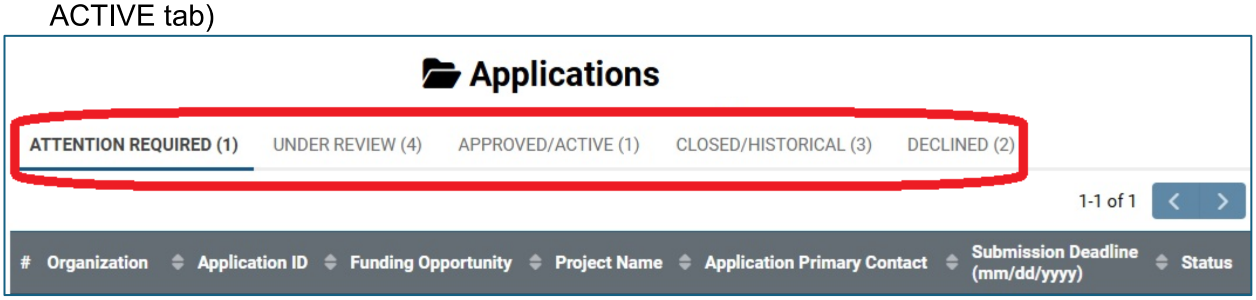
- **Attention Required** (information must be provided to move forward)
- **Under Review** (waiting for a decision)
- **Approved / Active** (currently receiving funding or reporting on these applications)
- **Closed / Historical** (past approved applications that are no longer active)
- **Declined**

ASSIGNING AND ADDING STAFF TO APPLICATIONS

Users cannot see any Application or its components (e.g., Reports) unless they are in the application's Contacts list.

Users can be added using the application's ***Manage Contacts*** and ***Revise Contacts*** areas.

1. On your home screen, find and select the Application (most likely in the APPROVED / ACTIVE tab)



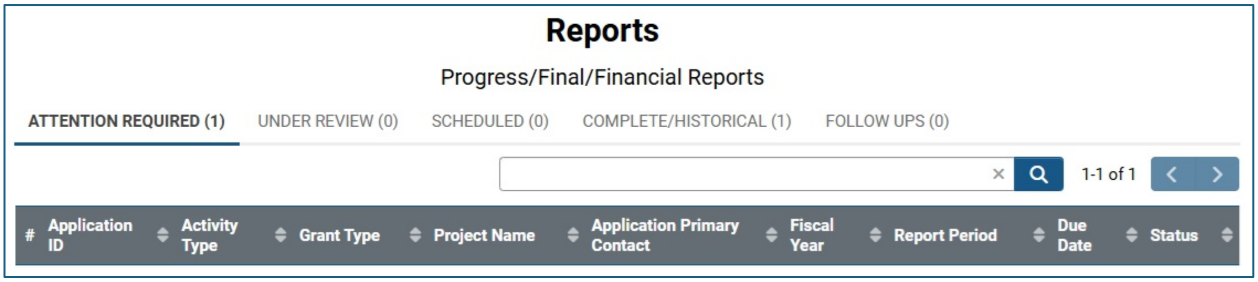
2. Select the "Organization" tab
3. Scroll to the bottom of the page or select ***Manage Contacts*** in the right-hand pop-out menu
4. Select ***Revise Contacts***
5. Select "Yes" or "No" regarding changing the Application Primary Contact
6. Select "Yes" or "No" regarding changing the Signing Authority
7. Scroll to the relevant ADD CONTACTS TO APPLICATION section
    a. Full
    b. Limited

8. Select the checkbox for each individual to be added
9. Select ***Apply Contact Changes / Save*** button

REPORTS

Reports are accessed from your home page.

1. On your home screen, scroll to the “Reports” section at the bottom of the page



2. You can search for the application ID number *or* select a report from the list
3. Reports are organized within one of multiple tabs, based on their current status. The number on the tab indicates the number of reports it holds.
    a. **Attention Required** (reports waiting for you to complete)
    b. **Under Review** (reports being reviewed by City Program Staff)
    c. **Scheduled** (upcoming reports that are not yet due)
    d. **Closed / Historical** (reports attached to applications that are no longer active)
    e. **Follow-ups** (City Program Staff have sent you a request for information)
4. The application ID number is noted in the first column
5. The “Reporting Period” and “Due Dates” are noted in columns 7 and 8
6. Select a report in the list to access it and submit your information

ONE STAGE APPLICATION WORKFLOW

➢ Full application is submitted and reviewed (e.g., Community Funding grants)

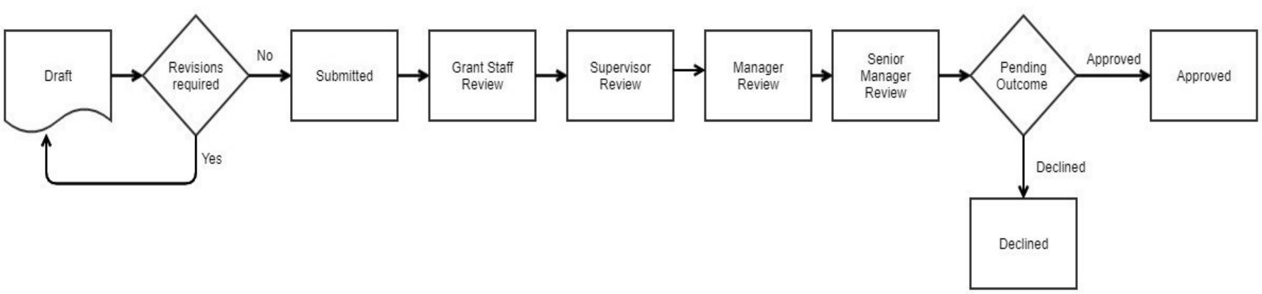


Figure 8 One-Stage application workflow

TWO STAGE APPLICATION WORKFLOW

- Eligibility to apply is completed prior to the full application being submitted for review (e.g., check to confirm educational institutions only apply for Student Nutrition Program funding)

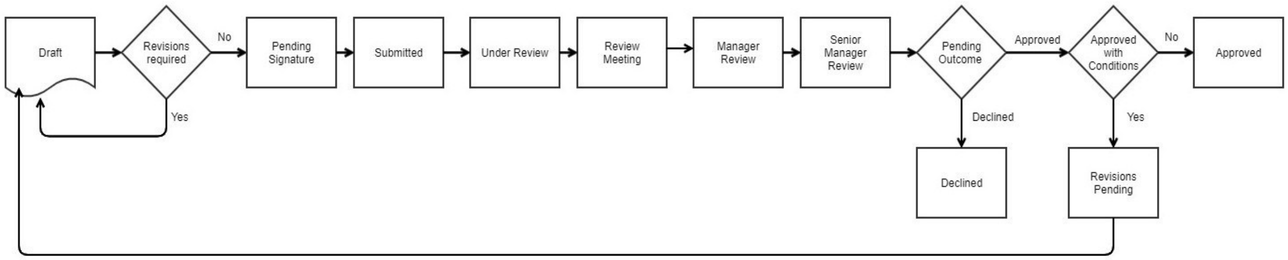


Figure 9 Two-Stage application workflow

APPENDIX A: TERMS AND CONDITIONS

SmartSimple External-Facing Services Policy

Your organization is responsible for ensuring that the data and/or information shared with the City have been collected in a manner that considers confidentiality, privacy and security, and is in conformity with all applicable laws.

All information your organization provides to the City of Toronto may be used and disclosed by the City for transparency and accountability purposes, in addition to the following activities:

- monitoring, evaluating, auditing and reporting on our applicants and grant recipients;
- conducting research, quality assurance, risk management and data analysis;
- supporting applicants and grantees to maximize their impact; and
- supporting learning opportunities through knowledge sharing.

By registering, providing information on your organization and/or submitting a grant application, your organization represents to the City that all such data and/or information has been collected by your organization in such a manner, and that the City has the permission of your organization and all relevant individuals to collect, use and disclose the data and/or information for the purpose of carrying out our mandate, including the activities described above.

APPENDIX B: SMARTSIMPLE CUSTOMER POLICY

Prohibited Uses

As a customer of SmartSimple, you may not use TGRIP to display, store, process or transmit, or permit use of TGRIP to display, store, process or transmit:

a. material that infringes or misappropriates a third-party's intellectual property or proprietary rights;
b. obscene, excessively profane material or otherwise objectionable material;
c. hate-related, bullying or violent material including material advocating discrimination or racial, religious or ethnic intolerance or material advocating or advancing computer hacking or cracking;
d. material related to phishing or drug paraphernalia;
e. malicious material;
f. unlawful software;
g. malicious code, such as viruses, worms, time bombs, Trojan horses and other harmful or malicious files, scripts, agents, or programs; or
h. material that violates or encourages conduct that would violate any applicable laws, including any criminal laws, or any third-party rights, including publicity or privacy rights.

Prohibited Actions

Customers of SmartSimple may not, and may not allow any third-party, including its users, to:

a. Generate or facilitate unsolicited commercial email (spam). Such prohibited activity includes, but is not limited to:
    i. imitating or impersonating SmartSimple, another person or his, her or its email address, or creating false accounts for the purpose of sending spam;
    ii. data mining or harvesting any web property (including any External-Facing Service) to find email addresses or other user account information;
    iii. sending unauthorized mail via open, third-party servers;
    iv. sending email to users who have requested to be removed from a mailing list;
    v. selling to, exchanging with, sharing with or distributing to a third-party personal information, including the email addresses of any person without such person's knowing and continued consent to such disclosure; or
    vi. sending unsolicited emails to significant numbers of email addresses belonging to individuals and/or entities with whom you have no pre-existing relationship;
    vii. sending communications or email in violation of applicable anti-spam laws or regulations within your jurisdiction;
b. send, upload, distribute or disseminate, or offer to do the same with respect to, unlawful, defamatory, harassing, abusive, fraudulent, infringing, obscene, excessively profane or otherwise objectionable material;
c. intentionally distribute viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive nature;
d. conduct or forward multi-level marketing, such as pyramid schemes and the like, or engage in, any unauthorized commercial purpose;
e. engage in phishing;

f. generate or facilitate SMS, MMS, or other text messages or push notifications in violation of any applicable laws including anti-spam, telemarketing or telephone consumer protection laws or regulations within your jurisdiction;
g. use of the External-Facing Services in any manner that violates any applicable industry standards, third-party policies or requirements that SmartSimple may communicate to its users, including all of the applicable guidelines published by accepted industry associations, carrier guidelines or other industry standards within your jurisdiction;
h. transmit material that may be harmful to minors;
i. illegally transmit another's intellectual property or other proprietary information without such owner's or licensor's permission;
j. impersonate another person, entity or SmartSimple (via the use of an email address or otherwise) or otherwise misrepresent themselves or the source of any email;
k. violate the rights (such as rights of privacy or publicity) of others;
l. promote or encourage illegal activity;
m. interfere with other users' enjoyment of an External-Facing Service;
n. engage in activity in connection with illegal peer-to-peer file sharing;
o. engage in or promote gambling, or run a gambling operation;
p. "mine" bitcoins and other cryptocurrencies;
q. sell, distribute or export prescription drugs or other controlled substances;
r. sell, distribute or promote drug paraphernalia;
s. access (including through any interfaces provided with an External-Facing Service), any SmartSimple product or service, or other service or website, in a manner that violates the terms for use of, or access to, such service or website;
t. operate an "open proxy" or any other form of Internet proxy service that is capable of forwarding requests to any end user or third party-supplied Internet host;
u. perform significant load or security testing without first obtaining SmartSimple's written consent;
v. remove any copyright, trademark or other proprietary rights notices contained in or on the Service or reformat or frame any portion of the web pages that are part of the
w. Service's administration display;
x. access a third-party web property for the purposes of web scraping, web crawling, web monitoring, or other similar activity through a web client that does not take commercially reasonable efforts to identify itself via a unique User Agent string describing the purpose of the web client and obey the robots exclusion standard (also known as the robots.txt standard), including the crawl-delay directive; or
y. use the External Facing Service in any manner that would disparage SmartSimple.